Technical Specification Group Services and System Aspects **TSGS#23(04)0320**
Meeting #24, Seoul, Korea 7-10 June 2004

Source: **TSG SA WG2**
Title: **CRs on 23.234 (3GPP WLAN interworking)**
Agenda Item: **7.2.3**

The following Change Requests (CRs) have been approved by TSG SA WG2 and are requested to be approved by TSG SA plenary #24.
Note: the source of all these CRs is now S2, even if the name of the originating company(ies) is still reflected on the cover page of all the attached CRs.

S2 doc #	Title	Spec	CR #	cat	Version in	REL	WI	S2 meeting	Clauses affected
S2-041642	Update of disconnection procedures	23.234	001r2	F	6.0.0	6	WLAN	S2 #39	7.4, 7.5, 7.6
S2-041215	Clarifications on the Wa reference point	23.234	012	F	6.0.0	6	WLAN	S2 #39	6.3.1.2
S2-041245	Corrections in the network selection clause	23.234	013r1	F	6.0.0	6	WLAN	S2 #39	5.4.2.1.3
S2-042236	Routing Enforcement in WLAN AN	23.234	022r2	F	6.0.0	6	WLAN	S2 #40	5.9, 6.2, 6.3
S2-041243	Corrections of Wg definition and some obsolete texts	23.234	027	F	6.0.0	6	WLAN	S2 #39	1, 3.2, 5.6.3
S2-042237	Update on definition on WLAN UE	23.234	029r2	F	6.0.0	6	WLAN	S2 #40	3.1, 6.2.1
S2-042318	Suggested changes to the new WLAN access terms	23.234	030r6	F	6.0.0	6	WLAN	S2 #40	3.1, 3.2, 4, 5.1, 5.2, 5.6, 5.7, 5.8, 5.9, 5.9.1, 5.9.2, 5.9.3, 5.9.4, 5.10, 5.11, 6.1.1, 6.1.2, 6.2.1, 6.2.2, 6.2.3, 6.2.5, 6.2.6, 6.3.6, 6.3.7, 6.3.8, 6.3.9, 6.3.10, 6.3.12, 7.3.1, 7.9, C.1, C.2.3, C.3, C.4, E.3, E.4
S2-042320	WLAN UE initiated disconnection procedures	23.234	033r3	F	6.0.0	6	WLAN	S2 #40	7
S2-042226	Clarification on WLAN access authentication and authorisation	23.234	035r2	F	6.0.0	6	WLAN	S2 #40	3.1, 6.2.5, 6.2.5.1,7.2
S2-041811	Reference to 23.825	23.234	036	F	6.0.0	6	WLAN	S2 #40	2, 6.2.6
S2-042219	Considerations on the format of the IP address used for tunnel establishment	23.234	038r2	F	6.0.0	6	WLAN	S2 #40	6.2.1, 6.2.6, 7.9, 7.9.3
S2-042225	Per-user charging in the VPLMN	23.234	041r2	F	6.0.0	6	WLAN	S2 #40	3.1, 6.2.2, 6.2.6, 6.3.6, 6.3.10, 6.3.11.2
S2-041862	Roaming access to WLAN local services in Scenario 2	23.234	043r2	C	6.0.0	6	WLAN	S2 #40	6.2.2, 6.3.1, 6.5, 7.2
S2-041851	Correction of Wd reference point requirements	23.234	044r1	F	6.0.0	6	WLAN	S2 #40	6.3.11
S2-041852	Clarification of Wm reference point	23.234	045r1	F	6.0.0	6	WLAN	S2 #40	6.3.10

	requirements								
S2-042283	Re-authentication	23.234	047r2	F	6.0.0	6	WLAN	S2 #40	7.9.1, 7.9.2
S2-042234	Alignment with 3GPP IMS architecture: SLF usage in Wx to locate the HSS	23.234	048r3	F	6.0.0	6	WLAN	S2 #40	2, 3.2, 5.1, 6.1.1, 6.1.2, 6.2.x (new), 6.3.x (new), 7.x (new)
S2-042235	Removal of WLAN UE classes	23.234	052r2	F	6.0.0	6	WLAN	S2 #40	6.2.1, 6.2.1.1
S2-042319	Merge of approved CR's in TS 23.234, Annex F	23.234	053r1	F	6.0.0	6	WLAN	S2 #40	F1, F2, F3, F4, F5
S2-042336	Combined CR to 23.234 Annex D (SMS over IP)	23.234	054r1	F	6.0.0	6	WLAN	S2 #40	Annex D

3GPP TSG-SA WG2 #39
Shenzhen, China, 19th – 23rd April 2004

Tdoc* ⌘ *S2-041642
revised s2-041203,S2-041238

CR-Form-v7

CHANGE REQUEST

⌘	**23.234**	**CR**	**001**	⌘**rev**	**2**	⌘	Current version:	**6.0.0**	⌘

For ***HELP*** *on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME □ Radio Access Network □ Core Network ☒

Title:	⌘	Update of disconnection procedures		
Source:	⌘	SA2 (Huawei, China Mobile)		
Work item code:	⌘	WLAN	***Date:*** ⌘	22/04/2004
Category:	⌘	**F**	***Release:*** ⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	In the TS 23.234 v6.0.0, the Procedure about disconnecting a subscriber from network are now only addressed the UEs only with the basic local access connections, the UEs which have the external IP network access connecion through the PDG are not considered, so the related tunel resource will not be released correctly..
Summary of change:	⌘	The process needed for the release of the external IP network access related resource and information are introduced in the network initiated disconnection procedures in section 7.4, 7.5 and 7.6.
Consequences if not approved:	⌘	In the case of network initiated disconnection, the tunnel related resorce and information for the external IP newwork access can not be correctly released.

Clauses affected:	⌘	7.4, 7.5, 7.6				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

*******************Change**********************

7.4 Cancelling WLAN Registration

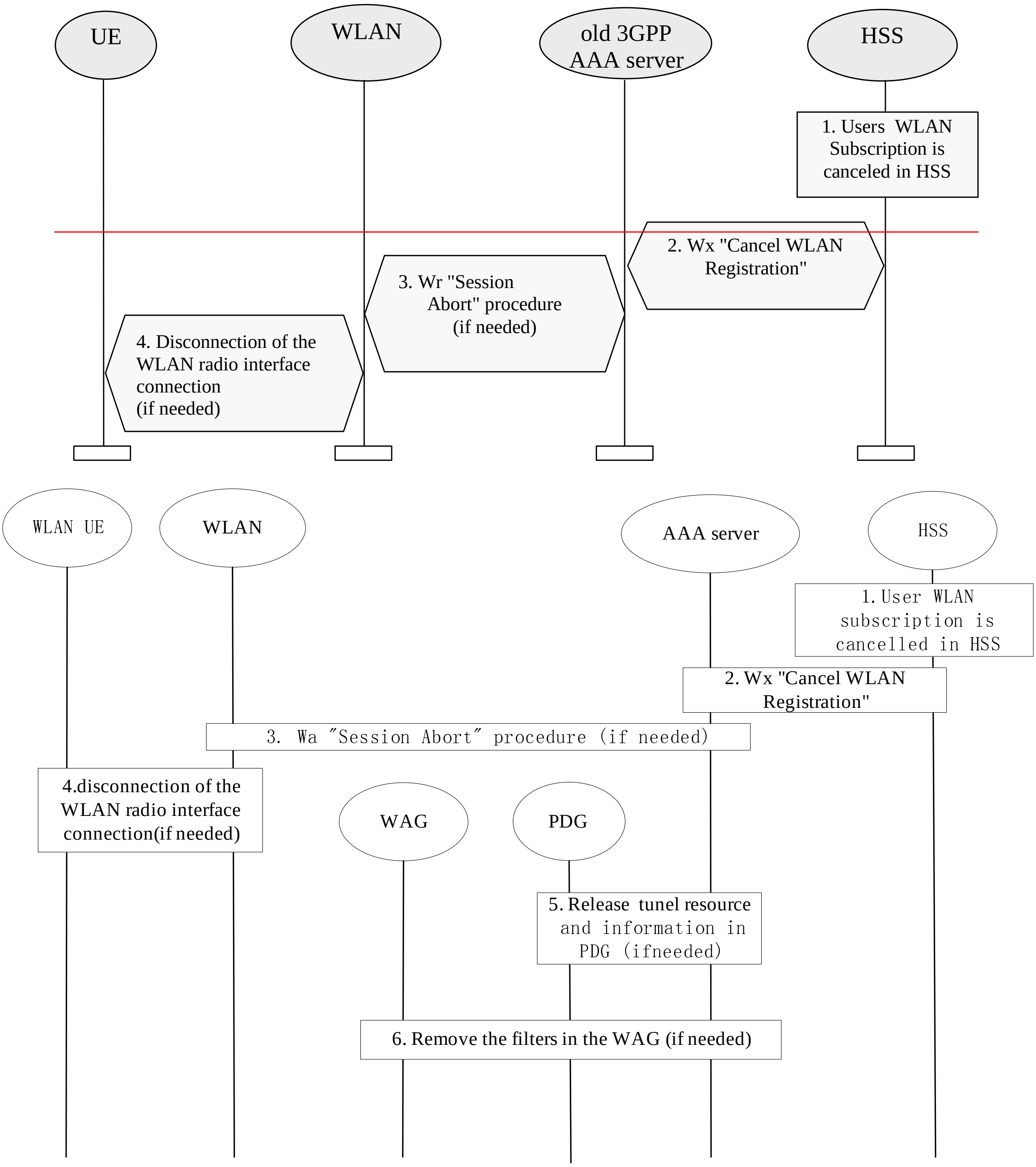

UE
WLAN
old 3GPP AAA server
HSS
1. Users WLAN Subscription is canceled in HSS
2. Wx "Cancel WLAN Registration"
3. Wr "Session Abort" procedure (if needed)
4. Disconnection of the WLAN radio interface connection (if needed)
WLAN UE
WLAN
AAA server
HSS
1. User WLAN subscription is cancelled in HSS
2. Wx "Cancel WLAN Registration"
3. Wa "Session Abort" procedure (if needed)
4.disconnection of the WLAN radio interface connection(if needed)
WAG
PDG
5. Release tunel resource and information in PDG (ifneeded)
6. Remove the filters in the WAG (if needed)

Figure 7.5: Cancellation of WLAN Registration Procedure

1. The 3GPP subscribers WLAN subscription is cancelled in HSS.

2. HSS cancels subscribers WLAN registration in the 3GPP AAA Server by Wx reference point procedure "Cancel WLAN Registration". In the messages subscriber is identified by his permanent identity.

3. If the subscriber's WLAN access connection still exists, Wa reference point procedure "Session Abort" procedure is executed towards WLAN.

4. If the radio connection still exists, WLAN disconnects the radio interface connection by WLAN technology specific mechanisms.

5．If the subscriber's tunnel connection with one or several PDG(s) exists, the 3GPP AAA server/proxy informs the PDG(s) over the Wm reference point, to remove the tunnel related information and resource.

6. The filters, which were deployed to WAG for the tunnel(s) during the tunnel establishment, are removed.

7.5 Disconnecting a Subscriber by WLAN

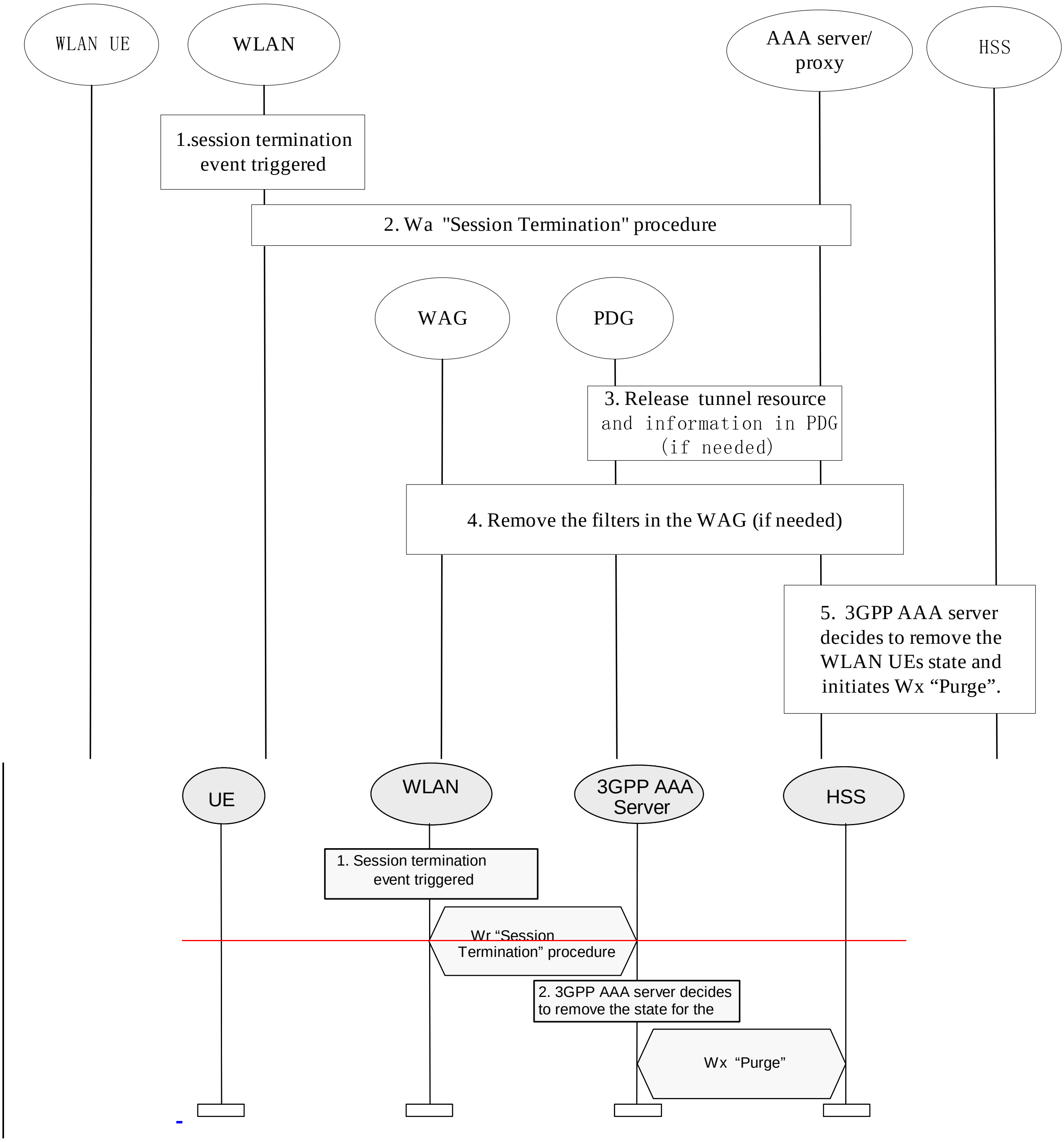

WLAN UE
WLAN
AAA server/ proxy
HSS
1.session termination event triggered
2. Wa "Session Termination" procedure
WAG
PDG
3. Release tunnel resource and information in PDG (if needed)
4. Remove the filters in the WAG (if needed)
5. 3GPP AAA server decides to remove the WLAN UEs state and initiates Wx "Purge".
UE
WLAN
3GPP AAA Server
HSS
1. Session termination event triggered
Wr "Session Termination" procedure
2. 3GPP AAA server decides to remove the state for the
Wx "Purge"

Figure 7.6: WLAN initiated disconnection procedure

1. WLAN detects that a Session related to a WLAN UE should be terminated towards the 3GPP AAA Server, e.g. when the WLAN UE has disappeared from WLAN coverage.

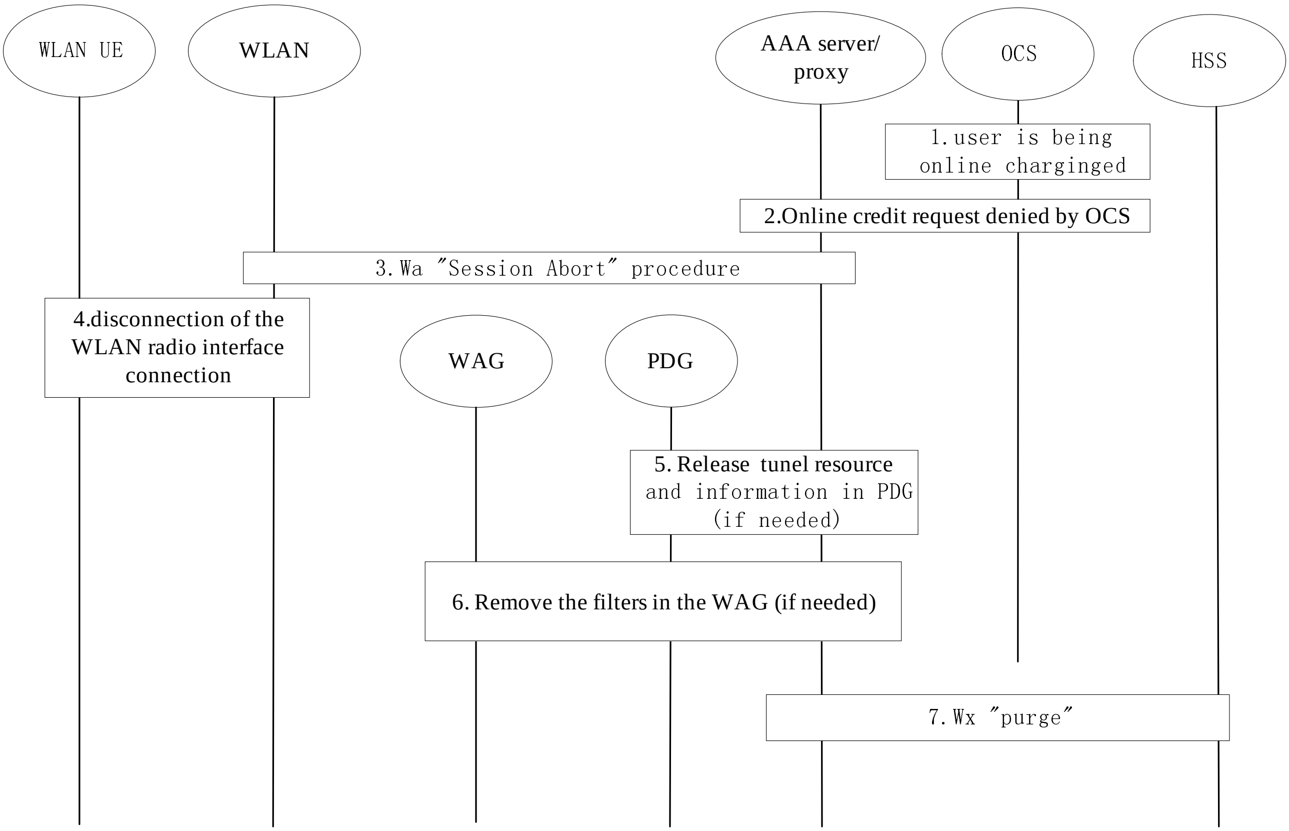
2. WLAN initiates Wa Session Termination procedure towards 3GPP AAA server.

3. If the subscriber has a tunnel connection with one or more PDGs, and the 3GPP AAA server/proxy needs to remove the connections, it informs the PDG(s) over the Wm reference point to remove the tunnel related information and resource.

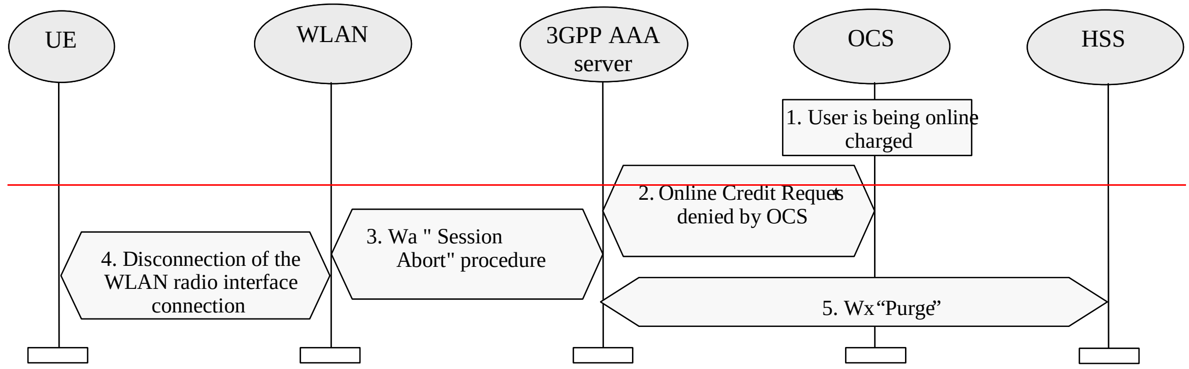
4. The filters, which were deployed to WAG for the tunnel(s) during the tunnel establishment, are removed.

5. In case when the 3GPP AAA server decides to remove the WLAN UEs state from the 3GPP AAA server, the 3GPP AAA server notifies HSS using Wx procedure "Purge" that the WLAN registration in the 3GPP AAA Server has been cancelled. HSS removes the state related to that 3GPP AAA server, e.g., the address of the serving 3GPP AAA server for the identified subscriber.

7.6 Disconnecting a Subscriber by Online Charging System



WLAN UE
WLAN
AAA server/ proxy
OCS
HSS
1.user is being online chargingeed
2.Online credit request denied by OCS
3.Wa "Session Abort" procedure
4.disconnection of the WLAN radio interface connection
WAG
PDG
5.Release tunel resource and information in PDG (if needed)
6.Remove the filters in the WAG (if needed)
7.Wx "purge"



UE
WLAN
3GPP AAA server
OCS
HSS
1. User is being online charged
2. Online Credit Requets denied by OCS
3. Wa " Session Abort" procedure
4. Disconnection of the WLAN radio interface connection
5. Wx"Purge"

Figure 7.7: OCS Initiated Disconnection Procedure

1. A subscriber is being online charged by 3GPP AAA server for WLAN access.

2. OCS (online Charging System) denies credit request from the 3GPP AAA server for WLAN access. The possibly already retrieved online credit runs out.

3. To disconnect the subscriber's connection, Wa reference point procedure "Session Abort" procedure is executed towards WLAN.

4. WLAN disconnects the radio interface connection by WLAN technology specific mechanisms.

5. If the subscriber's tunnel connection with one or several PDG(s) exists, the 3GPP AAA server/proxy informs the PDG(s) over the Wm reference point, to remove the tunnel related information and resource.

6. The filters, which were deployed to WAG for the tunnel(s) during the tunnel establishment, are removed.

7. If no Wx "Purge" procedure was already initiated in step 3, then the 3GPP AAA server notifies HSS that WLAN registration in the 3GPP AAA server has been cancelled by means of Wx procedure "Purge".

3GPP TSG-SA2 Meeting #39
Shenzhen, China, 19-23 April 2004

Tdoc ⌘ S2-041215

CR-Form-v7

CHANGE REQUEST

⌘	**23.234**	**CR**	**012**	⌘ **rev**	**-**	⌘	Current version:	**6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME □ Radio Access Network □ Core Network ☒

Title: ⌘	Clarifications on the Wa reference point		
Source: ⌘	SA2 (Nokia)		
Work item code: ⌘	WLAN	***Date:*** ⌘	19/04/2004
Category: ⌘	**F**	***Release:*** ⌘	Rel-6
	Use one of the following categories: ***F*** *(correction)* ***A*** *(corresponds to a correction in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)* Detailed explanations of the above categories can be found in 3GPP TR 21.900.		*Use one of the following releases:* *2 (GSM Phase 2)* *R96 (Release 1996)* *R97 (Release 1997)* *R98 (Release 1998)* *R99 (Release 1999)* *Rel-4 (Release 4)* *Rel-5 (Release 5)* *Rel-6 (Release 6)*

Reason for change: ⌘	It has been agreed and included in several parts of the specification that online charging shall be supported by the WLAN interworking architecture. The support of this functionality is not expressed in the description of the Wa reference point.
Summary of change: ⌘	This CR proposes the inclusion of the support of online charging functionality in the description of Wa reference point.
Consequences if not approved: ⌘	The specification remains ambiguous in terms of the role of the Wa reference point in supporintg online charging.

Clauses affected: ⌘	6.3.1.2			
	Y	**N**		
Other specs affected: ⌘		X	Other core specifications	⌘
		X	Test specifications	
		X	O&M Specifications	
Other comments: ⌘				

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

6.3.1 Wa reference point

6.3.1.1 General description

The Wa reference point connects the WLAN Access Network, possibly via intermediate networks, to the 3GPP Network (i.e. the 3GPP AAA Proxy in the roaming case and the 3GPP AAA server in the non-roaming case). The prime purpose of the protocols crossing this reference point is to transport authentication, authorization and charging-related information in a secure manner. The reference point has to accommodate also legacy WLAN Access Networks.

Legacy logical nodes outside of 3GPP scope that terminate or proxy the Wa reference point signalling and do not support 3GPP AAA protocol shall require signalling conversion between the legacy AAA protocol and the 3GPP AAA protocol.

EAP authentication shall be transported over the Wa reference point.

6.3.1.2 Functionality

The functionality of the reference point is to transport AAA frames:

- Carrying data for authentication signalling between WLAN UE and 3GPP Network.
- Carrying data for authorization signalling between WLAN AN and 3GPP Network. These data may include a well-defined identification of the WLAN AN.
- Carrying charging signalling per WLAN user. The data carried on the Wa interface shall enable both offline and online charging. To minimize the requirements put on the WLAN Access Network and to protect the confidentiality of the subscriber's charging status the fact whether a user is offline or online charged by his 3GPP subscription provider shall be transparent for the WLAN AN and thus for the Wa reference point.
- Enabling the identification of the operator networks amongst which the roaming occurs.
- Carrying keying data for the purpose of radio interface integrity protection and encryption.
- When such functionality is supported by the WLAN AN, purging a user from the WLAN access for immediate service termination

~~To minimize the requirements put on the WLAN Access Network and to protect the confidentiality of the subscriber's charging status the fact whether a user is offline or online charged by his 3GPP subscription provider shall be transparent for the WLAN AN and thus for the Wa reference point.~~

3GPP TSG-SA2 Meeting #39
Shenzhen, China, 19-23 April 2004

Tdoc ⌘S2-041245

CR-Form-v7

CHANGE REQUEST

⌘	**23.234**	**CR**	**013**	⌘ **rev**	**1**	⌘	Current version:	**6.0.0**	⌘

For ***HELP*** *on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME □ Radio Access Network □ Core Network ☒

Title:	⌘	Corrections in the network selection clause		
Source:	⌘	SA2 (Nokia, Samsung)		
Work item code:	⌘	WLAN	***Date:*** ⌘	19/04/2004
Category:	⌘	**F** *Use one of the following categories:* ***F*** *(correction)* ***A*** *(corresponds to a correction in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)* Detailed explanations of the above categories can be found in 3GPP TR 21.900.	***Release:*** ⌘	Rel-6 *Use one of the following releases:* *2 (GSM Phase 2)* *R96 (Release 1996)* *R97 (Release 1997)* *R98 (Release 1998)* *R99 (Release 1999)* *Rel-4 (Release 4)* *Rel-5 (Release 5)* *Rel-6 (Release 6)*

Reason for change:	⌘	The current text on manual network selection contains unnecesary and misleading sentences. Moreover the text contains incorrect references.
Summary of change:	⌘	It makes the text of the manual selection simpler and corrects the references.
Consequences if not approved:	⌘	The specification of the manual selection remains misleading and there will be incorrect references in the network selection clause.

Clauses affected:	⌘	5.4.2.1.3				
		Y	**N**			
Other specs affected:	⌘		X	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text.   Delete those parts of the specification which are not relevant to the change request.

5.4.2.1.3 Network Selection

The WLAN UE shall store a list of Preferred SSIDs provided by the Home Network operator and shall also maintain a list of the user's Preferred SSIDs.

The Operator's preferred SSID list would be populated, for example, with the SSIDs commonly used by major hotspot operators with whom the Home Operator has a direct relationship.

In Manual mode the WLAN UE shall scan (passive scanning) for all available SSIDs in beacon channels it can discover. The WLAN UE may also probe (active scanning) for additional available SSIDs from each of the WLAN networks that it has discovered. ~~Details on the usage of preferred SSID lists during active scanning are included in 3GPP TS 24.234 [9].~~

Once a list of all available SSIDs has been obtained, the WLAN UE ~~selects an SSID following the procedure specified in 3GPP TS 24.234 [9] clause 5.2.1 and performs association with the particular access point using the Selected SSID.~~

~~The WLAN UE~~ shall obtain a list of available PLMNs from each SSID~~ it associates with according to procedure defined in clause 5.4.3~~. When a list of PLMNs has been obtained from all SSIDs it shall present them to the user ~~for the user~~ to select one. The WLAN UE shall then associate with the SSID that supports ~~that~~ the PLMN that is selected by the user.

In the automatic mode the procedure is as follows:

0. The WLAN UE scans for all available SSIDs. It is not required to continue the scanning after the highest priority SSID is found.

1. Start association and perform Network Discovery

   1a) If authentication to HPLMN succeeds (i.e. EAP-Success is received), then stop this procedure.

   1b) If Network Advertisement information is received (i.e. EAP-Identity/Request is received), then store the list and start again step 1.

   Repeat step1 for all available SSIDs following the order specified in the lists of 'Preferred SSIDs for WLAN access'.~~clause 5.2.1~~ If the scanning in step 0 was stopped due to the discovery of the highest priority SSID, but the HPLMN has not been found (e.g. because the SSID list is not updated or the selected SSID was a fake one), then the user should go back to step 0 and scan for all available SSIDs.

   Note that if an AP supporting HPLMN is found in the middle of the procedure, step 1a, then step 1 is stopped and association with the remaining available APs will not take place.

2. Use the lists of 'Preferred PLMNs for WLAN access' and the lists from step 1b) to ~~find the best match.~~ Select the best matching PLMN. Then ~~S~~select the WLAN AN~~AP~~ that supports the best match VPLMN. If more than one WLAN AN supports the best matched VPLMN, the WLAN AN having the highest priority SSID is selected.

3. Associate with the AP selected in step 2 and attempt authentication with the best match PLMN.A WLAN AN may indicate that it provides 3G interworking without the involvement of any other network than the WLAN AN.

If such an indication is provided by the WLAN AN and if the WLAN UE supports the indication, then the WLAN UE shall use it at SSID selection as defined in 3GPP TS 24.234 [9].

The above requirement may be met through explicit EAP-based procedures or through the generic Preferred SSID list procedures – for example Preferred SSID lists could include SSID formats defined by operators for the above purposes.

3GPP TSG-SA2 Meeting #40
Sophia Antipolis, France, 17th – 21st May 2004

Tdoc ⌘S2-042236

CR-Form-v7

CHANGE REQUEST

⌘	**23.234**	**CR**	022	⌘ **rev**	**2**	⌘	Current version:	**6.0.0**	⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘ Routing Enforcement in WLAN AN			
Source:	⌘ SA2 (Samsung)			
Work item code:	⌘ WLAN		***Date:*** ⌘	21/05/04
Category:	⌘ ***F***		***Release:*** ⌘	*Rel-6*

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	In Section 5.9.2, Routing Enforcement in the WLAN AN, it is mentioned that "packets to/from PDG has to be properly routed by WLAN AN". But it should have been as "to/from UE" as WLAN AN is connected to only UE and the packets to/from UE are the ones that needs to be routed. In Section 6.2 and 6.3, Policy/Routing Enforcement functionality is not discussed as part of AAA Server and AAA-Proxy and the Wa reference point. So these functionalities are added.
Summary of change:	⌘	Change 'PDG' to 'UE' for the entity being affected by routing enforcement in Section 5.9.2. Add Policy/Routing Enforcement functionality to sections about 3GPP AAA proxy, 3GPP AAA server and the Wa reference point.
Consequences if not approved:	⌘	The meaning of routing enforcement is misleadling. Policy/Routing Enfocement functionalies will be missed in AAA proxy/server and the Wa reference point.

Clauses affected:	⌘	5.9, 6.2, 6.3				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

******** FIRST MODIFIED SECTION ********

5.9 Routing Enforcement and Policy Enforcement in Scenario 3

5.9.1 Purpose for routing enforcement and policy enforcement

In order to ensure operator policies, e.g. QoS, Charging can be applied to user traffic, scenario 3 requires routing enforcement and policy enforcement to be implemented in the 3GPP-WLAN interworking system.

5.9.2 Routing Enforcement in the WLAN AN

Routing enforcement shall be used to ensure that all packets sent to/from the WLAN UE for 3G PS based service are routed to the interworking VPLMN (roaming case) or HPLMN (no roaming case). However, this routing enforcement shall not prevent a WLAN AN from routing non 3G PS based service traffic to another network (e.g. the Internet) other than a PLMN, when provision of such services (e.g. direct Internet access from the WLAN) is agreed between the WLAN and the PLMN.

When subscription limits a WLAN UE to exclusively access only 3GPP PS based service, the PLMN can indicate to the WLAN AN routing enforcement to ensure that all packets sent to/from the WLAN UE are routed to the interworking VPLMN (roaming case) or HPLMN (no roaming case).

If a WLAN UE user subscription allows a Scenario 3 user to access a Scenario 2 type of service (e.g. direct internet access), the WLAN AN should be capable of routing packets directly to the external packet data network.

Routing enforcement in the WLAN AN shall ensure that packets sent ~~to/from the PDG~~ between a PDG and a WLAN UE are routed to the right entity in the interworking VPLMN (roaming case) or HPLMN (no roaming case).

Routing enforcement should not prevent the WLAN AN from supporting scenario 2 WLAN UE or a scenario3 capable WLAN UE opting for a scenario2 type of direct internet access, and non 3G interworking WLAN terminals.

Routing enforcement should have minimal impact on the WLAN AN.

******** NEXT MODIFIED SECTION ********

6.2.2 3GPP AAA Proxy

The 3GPP AAA Proxy represents a proxying and filtering function that resides in the Visited 3GPP Network. The 3GPP AAA Proxy functions include:

- Relaying the AAA information between WLAN and the 3GPP AAA Server.
- Enforcing policies derived from roaming agreements between 3GPP operators and between WLAN operator and 3GPP operator
- Reporting per-user charging/accounting information to the VPLMN CCF/CGw for roaming users
- Service termination (O&M initiated termination from visited network operator)
- Protocol conversion when the Wa and Wd reference points do not use the same protocol

For Scenario 3 only:

- Receiving authorization information related to subscriber requests for W-APNs in the Home or Visited network
- Authorization of access to Visited network W-APNs according to local policy
- Receiving the suitable policy enforcement information from AAA-Server and provides it to the WAG in VPLMN.
- May provide suitable routing enforcement information to WLAN AN.

The 3GPP AAA Proxy functionality can reside in a separate physical network node, it may reside in the 3GPP AAA Server or any other physical network node.

6.2.3 3GPP AAA Server

The 3GPP AAA server is located within the 3GPP network. The 3GPP AAA Server:

- Retrieves authentication information and subscriber profile (including subscriber's authorization information) from the HLR/HSS of the 3GPP subscriber's home 3GPP network.
- Authenticates the 3GPP subscriber based on the authentication information retrieved from HLR/HSS. The authentication signaling may pass through AAA proxies.
- Communicates authorization information to the WLAN potentially via AAA proxies.
- Registers its (the 3GPP AAA server) address or name with the HLR/HSS for each authenticated and authorized 3GPP subscriber.
- Initiates the Purge procedure when the 3GPP AAA server deletes the information of a subscriber.
- May act also as a AAA proxy (see above).
- Maintains the WLAN UE's WLAN-attach status.
- Provides the WLAN UE's WLAN-attach status to other entities (which are out of the scope of this TS).
- Generates and reports per-user charging/accounting information to the HPLMN CCF/CGw.

For scenario 3:

- Communicates service authorization information (e.g. authorized W-APN, necessary keying material for tunnel establishment and user data traffics) to the PDG. AAA proxies if the PDG is located in VPLMN.
- Provides the AAA-Proxy with suitable policy enforcement information.
- Provides suitable policy enforcement information to WAG in HPLMN.
- May provide suitable routing enforcement information to WLAN AN.

******** NEXT MODIFIED SECTION ********

6.3.1 Wa reference point

6.3.1.2 Functionality

The functionality of the reference point is to transport AAA frames:

- Carrying data for authentication signalling between WLAN UE and 3GPP Network.
- Carrying data for authorization signalling between WLAN AN and 3GPP Network. These data may include a well-defined identification of the WLAN AN.
- Carrying charging signalling per WLAN user.
- Enabling the identification of the operator networks amongst which the roaming occurs.
- Carrying keying data for the purpose of radio interface integrity protection and encryption.
- May carry Routing Enforcement information from the PLMN to ensure that all packets sent to/from the WLAN UE for PS based services are routed to the interworking VPLMN (roaming case) or HPLMN (no roaming case) appropriately.

- When such functionality is supported by the WLAN AN, purging a user from the WLAN access for immediate service termination

To minimize the requirements put on the WLAN Access Network and to protect the confidentiality of the subscriber's charging status the fact whether a user is offline or online charged by his 3GPP subscription provider shall be transparent for the WLAN AN and thus for the Wa reference point

******** END OF CHANGES ********

3GPP TSG-SA WG2 #39 **Tdoc ⌘S2-041243**
Shenzhen, China, 19th – 23rd April 2004

CR-Form-v7

CHANGE REQUEST

⌘ **23.234** **CR** **027** ⌘**rev** **-** ⌘ Current version: **6.0.0** ⌘

For ***HELP*** *on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME □ Radio Access Network □ Core Network ☒

Title:	⌘	Corrections of Wg definition and some obsolete texts		
Source:	⌘	SA2 (Huawei)		
Work item code:	⌘	WLAN	***Date:*** ⌘	19/04/2004
Category:	⌘	**F**	***Release:*** ⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	1. In the definitin of Symbols, the Wg missed the AAA server as the end of the the reference point. 2.the "3GPP WLAN subsystem" is a obsoleted and incorrect term should be corrected 3. an wrong note for External IP Network selection should be removed
Summary of change:	⌘	1 the definition of the Wg corrected 2.the "3GPP WLAN subsystem" is replaced with" The 3GPP WLAN Interworking system" 3. an obsolete note for External IP Network selection is removed "(whether the request is sent to the WAG or to the PDG is FFS)"
Consequences if not approved:	⌘	Definition of Wg keep unclear and inconsistant in the TS, Wrong term used in the scope descripton of the TS. Wrong specification text for External IP Network selection.

Clauses affected:	⌘	1, 3.2, 5.6.3				
		Y	**N**			
Other specs Affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

******************First Change**********************

1 Scope

This document specifies system description for interworking between 3GPP systems and WLAN Local Area Networks (WLANs). The intent of 3GPP–WLAN Interworking is to extend 3GPP services and functionality to the WLAN access environment: ~~.~~the 3GPP WLAN I~~i~~nterworking ~~sub~~system. The 3GPP WLAN ~~sub~~Interworking system is assumed to provide bearer services for connecting a 3GPP subscriber via WLAN to IP based services compatible with those offered via PS domain.

This specification defines a 3GPP system and procedures for the following functionalities:

- Provide the interworking WLAN with a means of Access, Authentication and Authorisation (AAA) through the 3GPP System, which allows WLAN UEs to access WLAN and the locally connected IP network (e.g. Internet)

- Provide WLAN UEs with IP bearer capability to access PS based services which are provided by PLMN.

*****************The Second Change*******************

3.2 Symbols

For the purposes of the present document the following symbols apply:

D'	Reference point between a pre-R6 HSS/HLR and a 3GPP AAA Server
Gr'	Reference point between a pre-R6 HSS/HLR and a 3GPP AAA Server
Wa	Reference point between a WLAN Access Network and a 3GPP AAA Server/Proxy (charging and control signalling)
Wd	Reference point between a 3GPP AAA Proxy and a 3GPP AAA Server (charging and control signalling)
Wf	Reference point between a CGw/CCF and a 3GPP AAA Server/Proxy
Wg	Reference point between a 3GPP AAA Server/Proxy and WAG
Wi	Reference point between a Packet Data Gateway and an external IP Network
Wm	Reference point between a Packet Data Gateway and a 3GPP AAA Server
Wn	Reference point between a WLAN Access Network and a WLAN Access Gateway
Wp	Reference point between a WLAN Access Gateway and a Packet Data Gateway
Wo	Reference point between a 3GPP AAA Server and an OCS
Wu	Reference point between a WLAN UE and a Packet Data Gateway
Wx	Reference point between an HSS and a 3GPP AAA Server

******************The Third Change*********************

5.6.3 External IP Network selection

The WLAN UE can connect to different IP networks, including the Internet, an operator's IP network or an external IP network such as a corporate IP network. The user may indicate a preferred IP network with a requested WLAN Access Point Name (W-APN). The Requested W-APN may also indicate a point of interconnection to the external IP network (i.e. PDG).

A W-APN is indicated by the WLAN UE in the tunnel establishment procedure between the WLAN UE and a PDG ~~(whether the request is sent to the WAG or to the PDG is FFS)~~. It is then forwarded to the 3GPP AAA server/proxy in the same network as the PDG~~.~~.

3GPP TSG-SA2 Meeting #40
Sophia Antipolis, France, 17th – 21st May 2004

Tdoc ⌘S2-042237

CR-Form-v7

CHANGE REQUEST

⌘	**23.234**	**CR**	029	⌘**rev**	**2**	⌘	Current version:	**6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☐

Title:	⌘	Update on definition on WLAN UE		
Source:	⌘	SA2 (Samsung)		
Work item code:	⌘	WLAN	***Date:*** ⌘	21/05/04
Category:	⌘	***F***	***Release:*** ⌘	*Rel-6*

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	A CR against TS 23.002 containing a definition of a WLAN UE has been approved. TS 23.234 needs to be updated in line with this change.
Summary of change:	⌘	The definition of a WLAN UE is removed. The introduction sentence of WLAN UE is modifined in line with the new definition in TS 23.002.
Consequences if not approved:	⌘	Duplicated and different definitions in the two TSes will lead to confusion.

Clauses affected:	⌘	3.1, 6.2.1				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

******** FIRST MODIFIED SECTION ********

3.1 Definitions

Available SSID: It is an SSID that the WLAN UE has found after active and/or passive scanning which meets certain conditions as specified in IEEE 802.11 [19].

3GPP - WLAN Interworking: Used generically to refer to interworking between the 3GPP system and the WLAN family of standards**.** Annex B includes examples of WLAN Radio Network Technologies.

Environment: The type of area to be covered by the WLAN network of a 3GPP - WLAN interworking; e.g. public, corporate and residential.

External IP Network/External Packet Data Network: An IP network to which access may be provided through the 3GPP system, rather than directly from the WLAN AN. For example, the Internet, an operator's IP network or a 3rd party IP network such as a corporate IP network.

Home WLAN: The WLAN that is interworking with the HPLMN of the 3GPP - WLAN interworking user.

Interworking WLAN : WLAN that interworks with a 3GPP system**.**

I-WLAN selection: Procedure for the selection among the available I-WLAN APs

Offline charging: Offline charging mechanism is provided for collecting and forwarding charging information about occurred WLAN access resource and core network resource usage, etc without affecting the service rendered in real-time.

Online charging: Online charging mechanism is provided where the service rendered is affected in real-time and is required for a direct interaction with session/service control. This allows an online charged subscriber to access WLAN.

Policy Enforcement: In scenario 3, Policy Enforcement is implemented in a WAG to allow only authorized packets to/from a WLAN AN to pass through.

PS based services: In WLAN interworking, PS based service is a general term to refer to the services provided by a PLMN using IP bearer capability between WLAN UEs and the PLMN in scenario 3 and upwards. They include all services provided by 3G PS domain that use the IP bearer service, (e.g., IMS, Internet access, Corporate IP network access), and other services (e.g., SMS and LCS).

Requested W-APN: The W-APN requested by the user

Routing Enforcement: In scenario 3, Routing Enforcement ensures that all packets sent to/from the WLAN UE for 3G PS based service are routed to the interworking VPLMN (roaming case) or HPLMN (no roaming case). Routing Enforcement is implemented between a WLAN AN and a WAG.

Selected W-APN: The W-APN selected by the network as a result of the user request

Service Authorization: Authorization for a user to access the requested service according to the user's subscription.

Supported PLMN: A PLMN of a roaming partner (i.e. to which the WLAN operator has a direct roaming relationship).

Visited WLAN: An interworking WLAN that Interworks only with a visited PLMN.

W-APN: WLAN Access Point Name – identifies an IP network and a point of interconnection to that network (Packet Data Gateway)

WLAN coverage: an area where wireless local area network access services are provided for interworking by an entity in accordance with WLAN standards.

WLAN roaming: The ability for a 3GPP - WLAN interworking user (subscriber) to function in a serving WLAN different from the home WLAN

~~**WLAN UE:** The WLAN UE is the UE (equipped with UICC card including (U)SIM) utilized by a 3GPP subscriber to access the WLAN interworking.~~

WLAN UE's local IP address: An address that is necessary to deliver the packet to a WLAN UE in a WLAN AN. It identifies the WLAN UE in the WLAN AN. WLAN UE's local IP address may be translated by Network Address Translation prior to being received by the interworking function.

WLAN UE's remote IP address: An address used in the data packet encapsulated by the WLAN UE-initiated tunnel. It represents the identity of the WLAN UE in the network which the WLAN UE is accessing.

****** NEXT MODIFIED SECTION ******

6.2.1 WLAN UE

A WLAN UE is the User Equipment using a UICC card utilized by a 3GPP subscriber to access the WLAN AN for 3GPP interworking purpose. ~~A WLAN UE is the UE (equipped with UICC card including (U)SIM) utilized by a 3GPP subscriber to access the WLAN network for 3GPP interworking purpose.~~ A WLAN UE may include terminal types whose configuration (e.g. interface to a UICC), operation and software environment are not under the exclusive control of the 3GPP system operator, such as a laptop computer or PDA with a WLAN card, UICC card reader and suitable software applications.

The WLAN UE functions include:

- Associating to an I-WLAN.
- WLAN access authentication based on EAP methods.
- Selection of a suitable VPLMN in the roaming case.
- Building an appropriate NAI.
- Obtain a local IP address.
- Building an appropriate W-APN to be used in scenario 3.
- Request the resolution of a W-APN in scenario 3 to a PDG address.
- Establish a secure tunnel in scenario 3 to a PDG.
- Obtain a remote IP address to be used in scenario 3.
- Accessing services provided in the operators PS domain.

- Allowing users to select the type of network access, i.e.between direct access to external IP networks from the WLAN AN and network access through PLMN.

****** END OF CHANGES ******

3GPP TSG-SA WG2 #40
Antipolis, France, 17th – 21st May 2004

Tdoc ⌘S2-042318

CR-Form-v7

CHANGE REQUEST

⌘	**23.234**	**CR**	**030**	⌘**rev**	**6**	⌘ Current version:	**6.0.0** ⌘

For ***HELP*** *on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects:	UICC apps⌘	□	ME	□	Radio Access Network	□	Core Network	☒

Title:	⌘	Merged CR 002 (Remove the WLAN “scenarios” referred texts) and CR 018 (Clarification of Wm reference point)		
Source:	⌘	SA2 (T-Mobile, Huawei, Siemens, Lucent)		
Work item code:	⌘	WLAN	***Date:*** ⌘	19/05/2004
Category:	⌘	**F**	***Release:*** ⌘	Rel-6
		Use one of the following categories: ***F*** *(correction)* ***A*** *(corresponds to a correction in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)* Detailed explanations of the above categories can be found in 3GPP TR 21.900.		*Use one of the following releases:* *2 (GSM Phase 2)* *R96 (Release 1996)* *R97 (Release 1997)* *R98 (Release 1998)* *R99 (Release 1999)* *Rel-4 (Release 4)* *Rel-5 (Release 5)* *Rel-6 (Release 6)*

Reason for change:	⌘	Whilst working on 23.234, SA2 has found that the use of the “scenario” terminology has caused confusion. In addition, SA1 does not refer to the scenarios in TS 22.234. The term “External IP networks” has not been consistently used. Current TS 23.234 defines Wm as reference point between AAA server and PDG in the home network. But it is not clear that this reference point is also needed between AAA proxy and PDG in the visited network to provide local services. In figure 6.2b the reference point between AAA proxy and PDG is not labeled.
Summary of change:	⌘	Remove the WLAN “scenarios” referred texts, replace with proper wording for the TS: the definition for the new terms are added: **WLAN Direct IP Access:** Access to an IP network is direct from the WLAN. **WLAN 3GPP IP Access:** Access to an IP network via the 3GPP system. The scenario 2 is replaced by “WLAN Direct IP Access” and scenario 3 is replaced by “WLAN 3GPP IP Access”; Unnecessary refers to the scenario terms are removed. Clarify that Wm reference point is between AAA proxy and PDG in the visited network.
Consequences if	⌘	Obsolete terms widely used in the TS, cause confusion and different explanation

not approved:	of the TS. Incomplete description of Wm reference point.

Clauses affected:	⌘	3.1, 3.2, 4, 5.1, 5.2, 5.6, 5.7, 5.8, 5.9, 5.9.1, 5.9.2, 5.9.3, 5.9.4, 5.10, 5.11, 6.1.1, 6.1.2, 6.2.1, 6.2.2, 6.2.3, 6.2.5, 6.2.6, 6.3.6, 6.3.7, 6.3.8, 6.3.9, 6.3.10, 6.3.12, 7.3.1, 7.9, C.1, C.2.3, C.3, C.4, E.3, E.4				
		Y	**N**			
Other specs affected:	⌘	**X**		Other core specifications	⌘	TS 33.234
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

********** MODIFIED SECTION **********

3.1 Definitions

Available SSID: It is an SSID that the WLAN UE has found after active and/or passive scanning which meets certain conditions as specified in IEEE 802.11 [19].

3GPP - WLAN Interworking: Used generically to refer to interworking between the 3GPP system and the WLAN family of standards**.** Annex B includes examples of WLAN Radio Network Technologies.

Environment: The type of area to be covered by the WLAN network of a 3GPP - WLAN interworking; e.g. public, corporate and residential.

External IP Network/External Packet Data Network: An IP network to which access may be provided through the 3GPP system, rather than directly from the WLAN AN. For example, the Internet, an operator's IP network or a 3rd party IP network such as a corporate IP network.

Home WLAN: The WLAN that is interworking with the HPLMN of the 3GPP - WLAN interworking user.

Interworking WLAN : WLAN that interworks with a 3GPP system**.**

I-WLAN selection: Procedure for the selection among the available I-WLAN APs

Offline charging: Offline charging mechanism is provided for collecting and forwarding charging information about occurred WLAN access resource and core network resource usage, etc without affecting the service rendered in real-time.

Online charging: Online charging mechanism is provided where the service rendered is affected in real-time and is required for a direct interaction with session/service control. This allows an online charged subscriber to access WLAN.

Policy Enforcement: ~~In scenario 3,~~Policy Enforcement is implemented in a WAG to allow only authorized packets to/from a WLAN AN to pass through.

PS based services: In WLAN interworking, PS based service is a general term to refer to the services provided by a PLMN using IP bearer capability between WLAN UEs and the PLMN when WLAN 3GPP IP Access is used~~in scenario 3 and upwards~~. They include all services provided by 3G PS domain that use the IP bearer service, (e.g., IMS, Internet access, Corporate IP network access), and other services (e.g., SMS and LCS).

Requested W-APN: The W-APN requested by the user

Routing Enforcement: ~~In scenario 3,~~ Routing Enforcement ensures that all packets sent to/from the WLAN UE for 3G PS based service are routed to the interworking VPLMN (roaming case) or HPLMN (no roaming case). Routing Enforcement is implemented between a WLAN AN and a WAG.

Selected W-APN: The W-APN selected by the network as a result of the user request

Service Authorization: Authorization for a user to access the requested service according to the user's subscription.

Supported PLMN: A PLMN of a roaming partner (i.e. to which the WLAN operator has a direct roaming relationship).

Visited WLAN: An interworking WLAN that Interworks only with a visited PLMN.

W-APN: WLAN Access Point Name – identifies an IP network and a point of interconnection to that network (Packet Data Gateway)

WLAN 3GPP IP Access: Access to an IP network via the 3GPP system

WLAN coverage: an area where wireless local area network access services are provided for interworking by an entity in accordance with WLAN standards.

WLAN Direct IP Access: Access to an IP network is direct from the WLAN AN.

WLAN roaming: The ability for a 3GPP - WLAN interworking user (subscriber) to function in a serving WLAN different from the home WLAN

WLAN UE: The WLAN UE is the UE (equipped with UICC card including (U)SIM) utilized by a 3GPP subscriber to access the WLAN interworking.

WLAN UE's local IP address: An address that is necessary to deliver the packet to a WLAN UE in a WLAN AN. It identifies the WLAN UE in the WLAN AN. WLAN UE's local IP address may be translated by Network Address Translation prior to being received by the interworking function.

WLAN UE's remote IP address: An address used in the data packet encapsulated by the WLAN UE-initiated tunnel. It represents the identity of the WLAN UE in the network which the WLAN UE is accessing.

*********** MODIFIED SECTION ***********

3.2 Symbols

For the purposes of the present document the following symbols apply:

D'	Reference point between a pre-R6 HSS/HLR and a 3GPP AAA Server
Gr'	Reference point between a pre-R6 HSS/HLR and a 3GPP AAA Server
Wa	Reference point between a WLAN Access Network and a 3GPP AAA Server/Proxy (charging and control signalling)
Wd	Reference point between a 3GPP AAA Proxy and a 3GPP AAA Server (charging and control signalling)
Wf	Reference point between a CGw/CCF and a 3GPP AAA Server/Proxy
Wg	Reference point between a 3GPP AAA Proxy and WAG
Wi	Reference point between a Packet Data Gateway and an external IP Network
Wm	Reference point between a Packet Data Gateway and a 3GPP AAA Server or 3GPP AAA proxy
Wn	Reference point between a WLAN Access Network and a WLAN Access Gateway
Wp	Reference point between a WLAN Access Gateway and a Packet Data Gateway
Wo	Reference point between a 3GPP AAA Server and an OCS
Wu	Reference point between a WLAN UE and a Packet Data Gateway
Wx	Reference point between an HSS and a 3GPP AAA Server

*********** MODIFIED SECTION ***********

4 WLAN Radio networks interworking with 3GPP

This specification defines two new procedures in the 3GPP System:

- WLAN Access, Authentication and Authorisation, which provides for access to the WLAN and the locally connected IP network (e.g. Internet) to be authenticated and authorised through the 3GPP System. Access to a locally connected IP network from the WLAN, is referred to as WLAN Direct IP Access.

- ~~Access to External IP networks~~WLAN 3GPP IP Access, which allows WLAN UEs to establish connectivity with ~~an~~ External IP networks, such as 3G operator networks, corporate Intranets or the Internet via the 3GPP system~~from a suitable IP network.~~

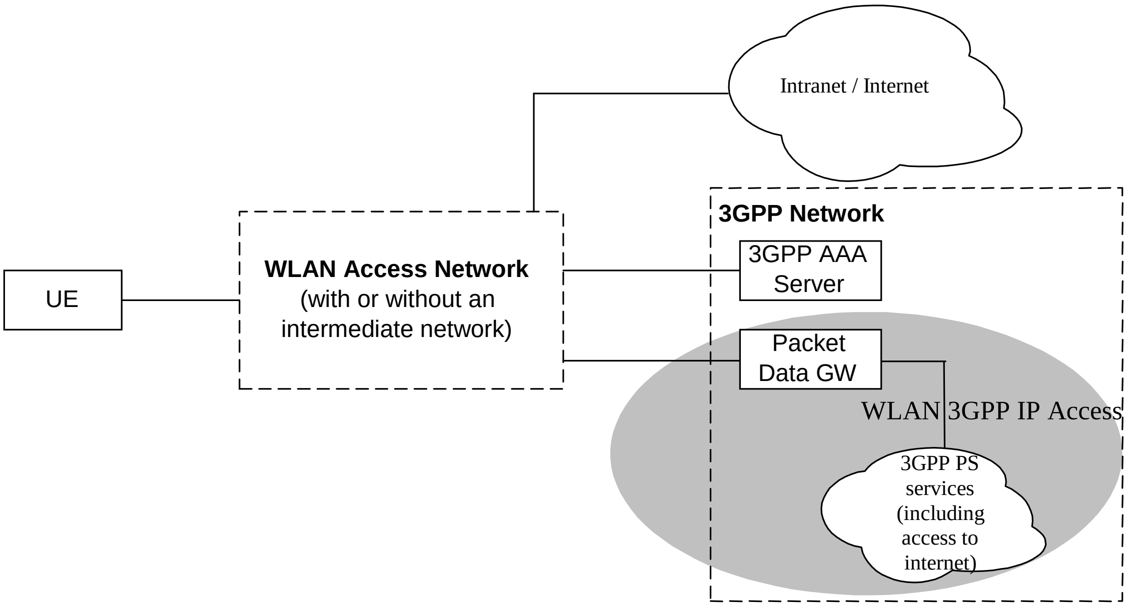
~~For scenario 3, access to External IP Networks~~WLAN 3GPP IP Access should, as far as possible, be technically independent of WLAN Access Authentication and Authorisation. However, ~~Access~~ WLAN 3GPP IP Access shall be possible only if WLAN Access Authentication/Authorisation has been completed first.

Note: The independence requirement does not preclude the possibility that the procedure ~~for access to external IP network~~WLAN GPP IP Access may rely on information derived in the procedure for WLAN Access Authorization.

~~Scenario 2 requires the first of these capabilities only. Scenario 3 requires a combination of both.~~

Figure 4.1 illustrates WLAN networks from the point of view of 3GPP interworking.

The Packet Data Gateway supports ~~access to External IP networks~~WLAN 3GPP IP Access ~~including those supporting 3GPP PS Domain based services~~ to External IP networks. ~~Scenario 2 offers direct connection from the WLAN to the Internet/intranet.~~ The WLAN includes WLAN access points and intermediate AAA elements. It may additionally include other devices such as routers. The WLAN User Equipment (WLAN UE) includes all equipment that is in possession of the end user, such as a computer, WLAN radio interface adapter etc.



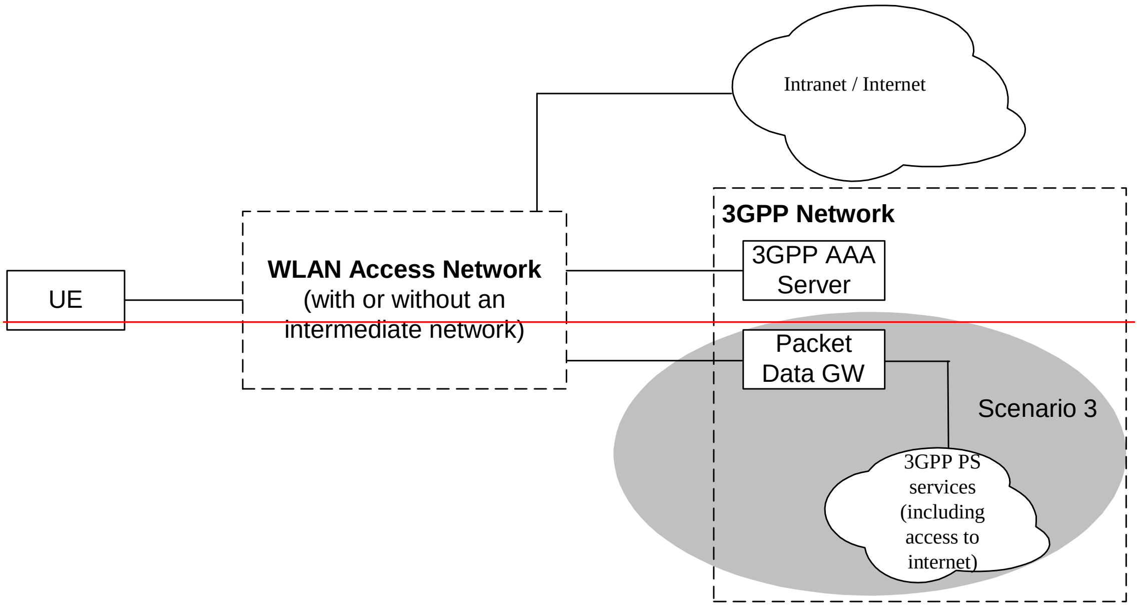


Figure 4.1: Simplified WLAN Network Model. The shaded area refers to WLAN 3GPP IP Access ~~scenario 3~~ functionality

As 3GPP-WLAN interworking concentrates on the interfaces between 3GPP elements and the interface between the 3GPP system and the WLAN, the internal operation of the WLAN is only considered in order to assess the impact of architecture options/requirements on the WLAN.

3GPP-WLAN interworking shall be independent of the underlying WLAN Radio Technology.

********** MODIFIED SECTION **********

5.1 Access Control Requirements

The following functional requirements have been identified:

- Legacy WLAN terminals should be supported. However software upgrades may be required for e.g. security reasons.
- Minimal impact on the user equipment, i.e. client software.
- Minimal impact on existing WLAN networks.
- The need for operators to administer and maintain end user software shall be minimized.
- Existing SIM and USIM shall be supported.
- Authentication shall rely on (U)SIM based authentication mechanisms.
- R6 USIM may include new functionality if necessary e.g. in order to improve privacy.
- Changes in the HSS/HLR/AuC shall be minimized.
- Methods for key distribution to the WLAN access network shall be supported.
- The WLAN connection established for a 3GPP subscriber shall have no impact to the capabilities of having simultaneous PS and CS connections for the same subscriber.
- WLAN Access Authorization shall occur upon the success of the authentication procedure. It shall take into account the user's subscription profile and optionally information about the WLAN AN, such as WLAN AN operator name, WLAN AN location information (e.g., country, telephone area code, city), WLAN AN throughput (e.g., maximum and minimum bandwidth guarantees for both ingress and egress traffic). This information is used to enable use-case scenarios like location based authentication/authorization, location based billing / customer care, and location based service offerings.
- It shall be possible to indicate to the user of the results of authorization requests.
- Results of WLAN Access Authorization requests shall be indicated to the WLAN, so that the WLAN can take appropriate action.
- The WLAN Access Authorization mechanism shall be able to inform the user and WLAN immediately of any change in service provision.
- This TS proposes solutions for operators who want to interwork their WLAN with an existing pre-R6 HLR/HSS.

Additional access control requirements for WLAN 3GPP IP Access~~scenario 3~~:

- Service Authorization shall occur after the WLAN Access Authentication/Authorization procedure.
- Service based policy control shall be possible for the services authorized for the user.
- Access to 3GPP PS based services shall be provided via WLAN. The interworking architecture shall be able to support all 3GPP PS based services.
- Access to PS based services normally provided by the 3GPP PS Core Network shall be provided via WLAN. WLAN access to these services shall support the same features as those supported via the 3GPP PS Core Network according to operator choice, e.g. private addressing schemes, external address allocation, secure tunneling to private external network. Quality of Service shall be supported when accessing these services via WLAN, although some limitations may exist because of the WLAN AN.

- A ~~scenario 3~~ WLAN inter-working system supporting both WLAN Direct IP Access and WLAN 3GPP IP Access shall be able to support WLAN UEs operating in the WLAN Direct IP Access mode only ~~scenario 2~~, e.g. according to subscription.

- A ~~Scenario3~~ combined access capable user should be able to choose between a ~~scenario2~~WLAN Direct IP Access only” ~~type of internet access (direct access through local network)~~ or a ~~scenario3~~ WLAN 3GPP IP Access ~~type of access to internet (through the PLMN)~~, when the network allows it.

- When the WLAN inter-working system does not support access to 3GPP PS based services, the WLAN UE shall be able to detect it.

- A WLAN 3GPP IP Access capable~~scenario 3~~ WLAN inter-working system shall be able to mandate all flows for 3G PS based services to be routed to the HPLMN or the VPLMN, e.g. according to subscription. This routing enforcement shall not rely on the WLAN UE client.

Note: This may mandate additional functionality existing in the WLAN AN

- The technical solution for access control to ~~External~~ local IP networks from WLAN shall be decoupled from WLAN Access Control.

********** MODIFIED SECTION **********

5.2 Access Control Principles

End to End Authentication: WLAN Authentication signaling is executed between WLAN UE and 3GPP AAA Server for the purpose of authenticating the end-user and authorizing the access to the WLAN and 3GPP network.

Transporting Authentication signalling over WLAN Radio Interface: WLAN authentication signalling is carried between WLAN UE and WLAN AN by WLAN Access Technology specific protocols. To ensure multivendor interoperability these WLAN technology specific protocols shall conform to existing standards of the specific WLAN access technology.

Transporting Authentication signalling between WLAN AN and 3GPP network: WLAN Authentication signalling shall be transported **between any WLAN AN and 3GPP network** by a standard protocol, which is independent of the specific WLAN technology utilised within the WLAN Access network.

Details of end to end authentication and transport of authentication signalling over the WLAN radio interface and between the 3GPP network and WLAN is covered in 3GPP TS 33.234 [10]

WLAN Access Authorization: This defines the process(es) in 3GPP AAA Server verifying whether WLAN Access should be allowed to a subscriber and deciding what access rules/policy should be applied to a subscriber. It is the stage after access authentication, but before service authorisation and WLAN UE's local IP address allocation.

After the authentication process succeeds, there could be additional conditions for the 3GPP AAA Server to decide whether the access is allowed and what access rules/policy should be applied. These conditions may be based on the subscriber's profile, the account status, O&M rules, local agreements or information about the WLAN AN.

The procedure for WLAN Access Authorization between the WLAN UE and the 3GPP AAA Server is combined with the WLAN Access Authentication.

Access rules/policy decided by the 3GPP AAA Server may be deployed in the 3GPP AAA Server, or/and in other entities such as the WAG or the WLAN AN.

Access rules/policy may include access scope limitation, time limitation, bandwidth control values, and/or user priority.

WLAN Access rules/policy should be specified by the home and/or visited operator based on the subscriber's profile, the account status, O&M rules (e.g. blacklist, access limitation list), and local agreements. Factors such as access time and access location could also be considered in these rules.

The access scope limitation could be, for example, only/not/may "access through WAG"; only/not/may "access intranet X".

Access scope limitation can be achieved using IP allocation scheme, VLAN allocation, Filtering, ACLs in the routers and switchers, etc.

Different access priority or the range of priorities may be authorized for different subscribers, and/or for one subscriber based on different access time or location, etc.

3GPP WLAN attach: The WLAN-attach status indicates whether the WLAN UE is now being served by the 3GPP WLAN IW network.

A WLAN UE is "WLAN-attached" after successful authentication and WLAN Access Authorization.

A WLAN UE is "WLAN-detached" in 3GPP network after its disconnection, or its authentication or WLAN Access Authorization being cancelled.

The WLAN-attach status is maintained by the 3GPP AAA server.

The WLAN UE's WLAN attach status should be obtained from the AAA Server directly or through the HSS, by other entities in the 3GPP or 3GPP connected network. Other entities in the 3GPP network obtain the WLAN UE's WLAN-attach status directly from the AAA Server or through the HSS. These entities and the corresponding reference points are not in the scope of this TS.

The description of the corresponding status in the WLAN UE is out of the scope of this TS.

Additional access control principles for ~~scenario 3~~WLAN 3GPP IP Access:

Service Selection and A~~a~~uthorisation: The solution shall include means for securely delivering service selection information from the WLAN UE to the 3GPP AAA server in the Home Network. If a ~~scenario3~~ user chooses to access the internet directly using the local IP network ~~(like a scenario2 user)~~, no service selection information is passed to the PLMN. In all other cases, where ~~a~~ WLAN 3GPP IP Access ~~scenario3~~ is desired~~type of services is opted by the user,~~, the service selection information shall contain ~~an~~ the name ~~indication of the requested~~of the W-APN to which access is requested. The 3GPP AAA Server in the Home network shall verify the users subscription to the indicated W-APN against the subscriber profile retrieved from HSS. The 3GPP AAA Server selects a W-APN based on the requested W-APN and on the user's subscription/local policy.

The service request shall be indicated by a tunnel establishment request from the WLAN UE to the PDG. The PDG shall then seek authentication/authorisation from the 3GPP AAA Proxy or Server in the same network.

The results of the authorisation decision shall be communicated to the Visited Network. All subscription-based authorisation decisions are made in the Home network.

In the case of a request for access to services provided in the Visited Network, the 3GPP AAA Proxy shall also authorise access based on local policy.

********** MODIFIED SECTION **********

5.6 Service Authorization Principles for ~~scenario 3~~WLAN 3GPP IP Access

The home network decides whether visited service is allowed or not based on e.g. W-APN, the user subscription information, visited network capabilities and roaming agreement.

5.6.1 Accessing Home Network provided services

The following functionality and requirements have been identified:

- It shall be possible to support multiple service authorizations after a successful WLAN authentication/authorisation (i.e. EAP success).
- The Service authorisation procedure should, as far as possible, be independent from WLAN Access authentication and authorisation.
- The routing policy applied at WLAN Access Authentication and Authorisation may include policy determining whether the user has IP connectivity to the PDGs used for access to external IP networks.
- It shall be possible to permit access to different services simultaneously.
- Service authorization information shall be protected
- The Access Point Name (APN) concept defined in 3GPP TS 23.003 shall be used for WLAN interworking authorization (namely W-APN). In a service authorization procedure:
    - W-APN selection and authorization is an end-to-end procedure between the WLAN UE and the HPLMN (the service authorization decision is made by the 3GPP AAA Server *based on subscription information retrieved from the HSS/HLR*).

Editor's note: the use of subscription information is FFS.

- The WLAN UE shall use W-APN to indicate to the network the service or set of services it wants to access.
- The PDG selection is under control of the 3GPP Home Network. The selection is based on the requested W-APN and user subscription information. The mechanism to select the PDG by the home network is out of scope of this specification, since it depends on the operator's preference.
- The PDG needs to know the authorized W-APN to select the external network, i.e. Wi interface.

5.6.2 Accessing Visited Network provided services

When accessing visited network provided services, additional principles below apply:

- In order for the WLAN UE to be able to use W-APNs in the VPLMN, the 3GPP AAA Server needs to pass to the 3GPP AAA Proxy the authorized W-APN and service related information which is required by the Visited Network to perform the service.
- The W-APN needs to be understood by both the Home and the Visited Networks.
- The V-PDG selection is under control of the 3GPP Visited Network. The selection is based on the authorized W-APN and service related information. The mechanism to select the V-PDG by the Visited Network is out of scope of this specification, since it depends on the operator's preference.
- The selected PDG in the Visited Network needs to know the authorized W-APN to select the external network, i.e. Wi interface.

5.6.3 External IP Network selection

The WLAN UE can connect to different External IP networks, such as~~including~~ the Internet, an operator's IP network or ~~an external IP network such as~~ a corporate IP network. The user may indicate a preferred IP network with a requested WLAN Access Point Name (W-APN). The Requested W-APN may also indicate a point of interconnection to the external IP network (i.e. PDG).

A W-APN is indicated by the WLAN UE in the tunnel establishment procedure between the WLAN UE and a PDG (whether the request is sent to the WAG or to the PDG is FFS). It is then forwarded to the 3GPP AAA server/proxy *in the same network as the PDG.*.

5.7 IP Connectivity for WLAN 3GPP IP Access ~~scenario 3~~

5.7.1 Principles

The WLAN UE initiates the establishment of tunnels and is involved in packet encapsulation/decapsulation. The tunnel shall reside between the WLAN UE and the PDG. In the non roaming case, the PDG shall reside in the Home PLMN; in the roaming case, the PDG may reside either in the Home or in the Visited PLMN (both cases shall be supported).

The following steps are performed after WLAN access authentication/authorisation:

1. W-APN resolution and discovery of the tunnel endpoint (PDG) IP-address is performed using the procedures described in clause 7.9.

2. Tunnel establishment, including mutual authentication, shall occur between the WLAN UE and the PDG.

Note 1: Filtering attributes may be needed in order to enable the WLAN to enforce that the WLAN UE tunnels all traffic as required. Filtering attributes may be transmitted from 3GPP AAA Server to WLAN over the Wa reference point. The WLAN Access Network sets up appropriate packet filters.

Note 2: The PDG is described in section 6.

The tunnel establishment is not coupled to WLAN access authentication/authorisation. The WLAN UE may establish several tunnels in order to access several external IP networks simultaneously. The external IP network selection is performed as part of the establishment of each tunnel.

Editor's note: Routing towards the Home PLMN in the Visited PLMN, as well as its impacts on the WLAN AN, are for further study.

5.7.2 Tunnelling Requirements

The requirements that a WLAN UE-Initiated tunnelling protocol should meet are:

- Minimal requirements to the underlying IP connectivity network, i.e. WLAN UE initiated tunnelling and tunnel establishment signalling can be deployed on top of generic IP connectivity networks
- Minimal impacts to the WLAN Access Network
- Establishment of trusted relationships (e.g. mutual authentication for both tunnel end-points) shall be possible
- Tunnel IP configuration of the WLAN UE may be obtained from/through the remote tunnel endpoint
- Set up secure tunnels between WLAN UE and remote tunnel endpoint. Especially support encryption and integrity protection during tunnel establishment and while transporting user data packets, if enabled.
- Remote IP address (inner IP):
  - The transport of IPv4 packets shall be supported
  - The transport of IPv6 packets shall be supported (e.g. in order to support IPv6 services like IMS)
- Local IP address (outer IP):
  - The tunnel protocol shall be able to support IPv4 and IPv6 transport addresses
  - The tunnel protocol shall support private WLAN UE's local IP addresses, which are non-routable in the public Internet..
- The protocol should be fully specified and 3GPP should define its usage to enable multi-vendor inter-operability.

5.8 Roaming requirements for WLAN 3GPP IP Access ~~scenario 3~~

For the delivery of 3GPP PS based services in a roaming scenario:

- The roaming architecture shall ensure that CDRs can be generated e.g. volume and time based by the visited network.
- The roaming architecture shall ensure that tunnels established are between entities that have a roaming agreement.
- The roaming architecture shall ensure that the bearer path from the WLAN to Home/Visited 3GPP network conforms to QoS and roaming agreement(s).
- The roaming architecture shall provide the ability to allow the user to access services provided by the visited network, e.g. local PS services.
- The roaming architecture shall allow the home network to limit the set of 3GPP services available for a given roaming user.
- ~~Scenario 3 requires that a~~All packets of PS based services sent to/from a WLAN UE are routed via a VPLMN in a 3GPP network, however basic Internet access may be routed directly from the WLAN.

5.9 Routing Enforcement and Policy Enforcement ~~in~~for WLAN 3GPP IP Access~~Scenario 3~~

5.9.1 Purpose for routing enforcement and policy enforcement

In order to ensure operator policies, e.g. QoS, Charging can be applied to user traffic, WLAN 3GPP IP Access~~ scenario 3~~ requires routing enforcement and policy enforcement to be implemented in the 3GPP-WLAN interworking system.

5.9.2 Routing Enforcement in the WLAN AN

Routing enforcement shall be used to ensure that all packets sent to/from the WLAN UE for 3G PS based service are routed to the interworking VPLMN (roaming case) or HPLMN (no roaming case). However, this routing enforcement shall not prevent a WLAN AN from routing non 3G PS based service traffic to another network (e.g. the Internet) other than a PLMN, when provision of such services (e.g. direct Internet access from the WLAN) is agreed between the WLAN and the PLMN.

When subscription limits a WLAN UE to exclusively access only 3GPP PS based service, the PLMN can indicate to the WLAN AN routing enforcement to ensure that all packets sent to/from the WLAN UE are routed to the interworking VPLMN (roaming case) or HPLMN (no roaming case).

If a WLAN UE user subscription allows a WLAN Direct IP Access~~Scenario 3 user to access a Scenario 2 type of service (e.g. direct internet access),~~ the WLAN AN should be capable of routing packets directly to the external packet data network.

Routing enforcement in the WLAN AN shall ensure that packets sent to/from the PDG are routed to the right entity in the interworking VPLMN (roaming case) or HPLMN (no roaming case).

Routing enforcement should not prevent the WLAN AN from supporting a~~scenario 2 ~~ WLAN Direct IP Access only capable WLAN UE or a WLAN 3GPP IP Access~~scenario3~~ capable WLAN UE opting for a WLAN Direct IP Access~~scenario2 type of direct internet access~~, and non 3G interworking WLAN terminals.

Routing enforcement should have minimal impact on the WLAN AN.

5.9.3 Routing enforcement and policy Enforcement in the HPLMN

When ~~operating in scenario 3~~supporting WLAN 3GPP IP Access and access is via a tunnel endpoint (PDG) in the HPLMN, the HPLMN shall be able to provide the VPLMN with suitable policy enforcement information. The HPLMN may also provide suitable routing enforcement information to WLAN.

5.9.4 Routing enforcement and policy Enforcement in the VPLMN

When ~~operating in~~ supporting WLAN 3GPP IP Access~~scenario 3~~, the VPLMN shall be able to implement policy enforcement on traffic sent to/from a WLAN UE according to policy enforcement information provided by the HPLMN.

The VPLMN may also provide suitable routing enforcement information to WLAN.

5.10 IP address allocation for the WLAN UE

When using ~~In Scenario 2~~WLAN Direct IP Access, a WLAN UE needs to use its local IP address only. ~~In~~ When using WLAN 3GPP IP Access~~Scenario 3~~, a WLAN UE shall use two IP addresses; its local IP address and remote IP address.

A WLAN UE's local IP address identifies the WLAN UE in the WLAN AN. In systems supporting only WLAN Direct IP Access ~~scenario 2~~, the WLAN UE's local IP address is assigned by the WLAN AN; in a WLAN 3GPP IP Access enabled system~~scenario 3~~, it can be assigned by a WLAN or by a PLMN (a VPLMN in roaming case and a HPLMN in non-roaming case). For the WLAN-assigned local IP address, which belongs to the address space of WLAN AN, there is no additional requirement on the WLAN. WLAN UE's local IP address allocation by the PLMN is for further study.

~~In~~ When using WLAN 3GPP IP Access~~scenario 3~~, a WLAN UE's remote IP address identifies the WLAN UE in the network that the WLAN UE is accessing for the 3G PS service. It shall be used for the inner packet of the WLAN UE-initiated tunnel. It can be assigned by HPLMN, VPLMN or an external IP network. The only case where VPLMN assigns the remote IP address for the WLAN UE is when the WLAN UE-initiated tunnel terminates at the VPLMN's PDG. When the WLAN UE's remote IP address is allocated by the external IP network, the PDG is required to have an interface with an address allocation server, such as AAA or DHCP, belonging to the external IP network. For the WLAN UE's remote IP address, IPv4 addresses shall be supported. When the WLAN UE accesses 3G PS based services using an IPv6 network such as IMS services, IPv6 addresses shall be supported for the WLAN UE's remote IP address. To avoid any clashes between addresses used in WLAN AN and PLMN and to enable correct routing of packets sent out by the WLAN UE the PLMN operator should allocate public addresses to network nodes, which are addressed by WLAN UEs.

When a WLAN UE accesses several 3G PS based services with different W-APNs simultaneously, the WLAN UE can get several remote IP addresses. There may be several WLAN UE-initiated tunnels for the services.

5.11 Charging

The following functionality and requirements have been identified:

- The WLAN Access Network shall be able to report the WLAN access usage to the appropriate 3GPP system (i.e. VPLMN in the roaming case and HPLMN in the non-roaming case).

- It shall be possible for the 3GPP system to control a specific ongoing WLAN access session for online charging purposes.

- It shall be possible for an operator to maintain a single prepaid account for WLAN, PS, CS, and IMS for a user.

- The 3GPP system shall be able to process the WLAN access resource usage information, and convert it into the format used in 3GPP networks (e.g. CDR).

- It shall be possible to correlate charging and accounting records generated in WLAN Access related nodes and records generated in 3GPP nodes.

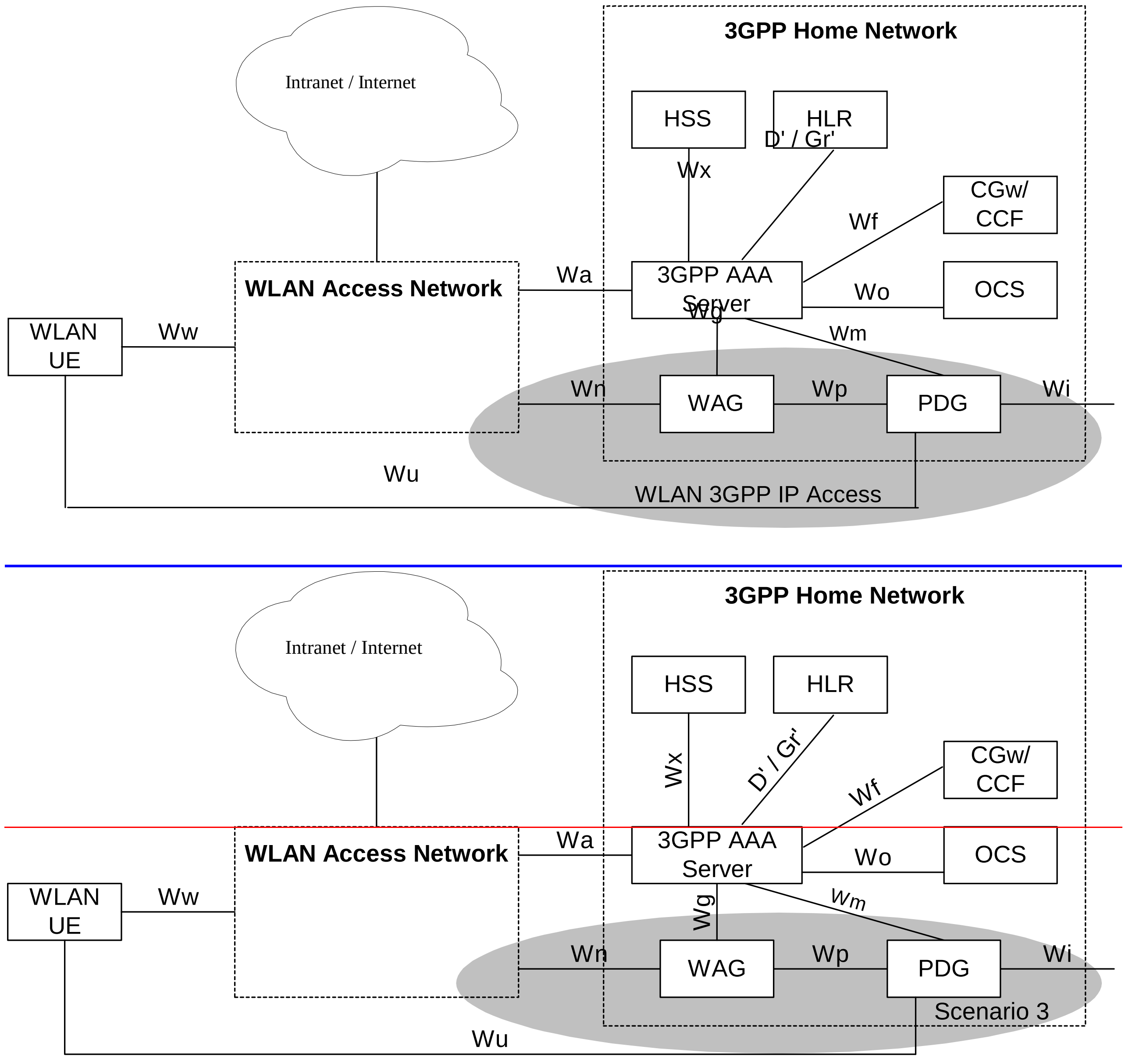
- It shall be possible to apply offline charging and online charging mechanisms for the WLAN interworking with 3GPP network.

Additionally, f~~F~~or WLAN 3GPP IP Access~~Scenario 3~~:

- It shall be possible to generate per user charging information in the HPLMN and in the VPLMN irrespective of whether the service is provided in the HPLMN or in the VPLMN.

********** MODIFIED SECTION **********

6.1.1 Non Roaming WLAN Inter-working Reference Model



Note: The shaded area refers to WLAN 3GPP IP Access~~scenario 3~~ functionality.

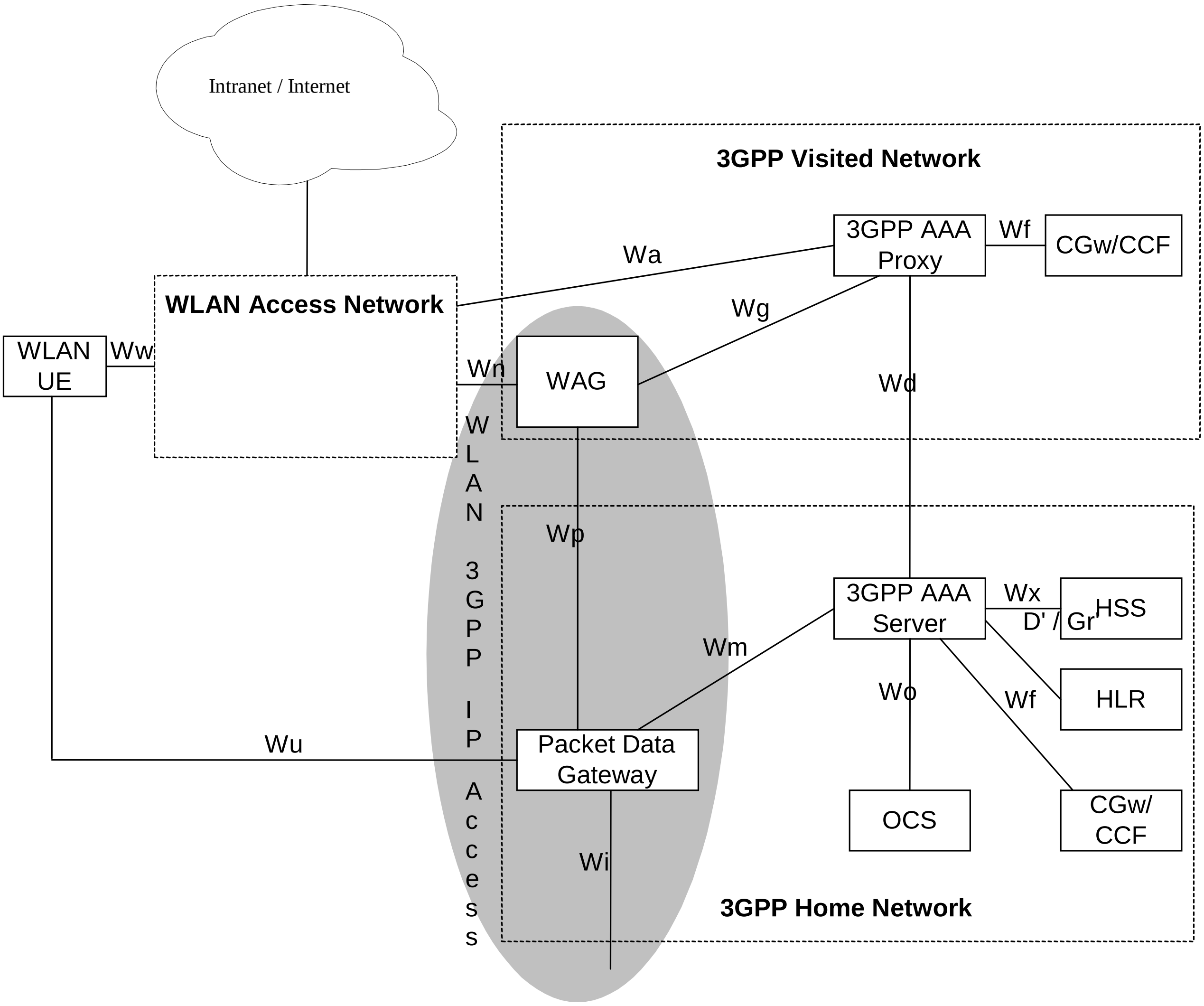
Figure 6.1: Non-roaming reference model

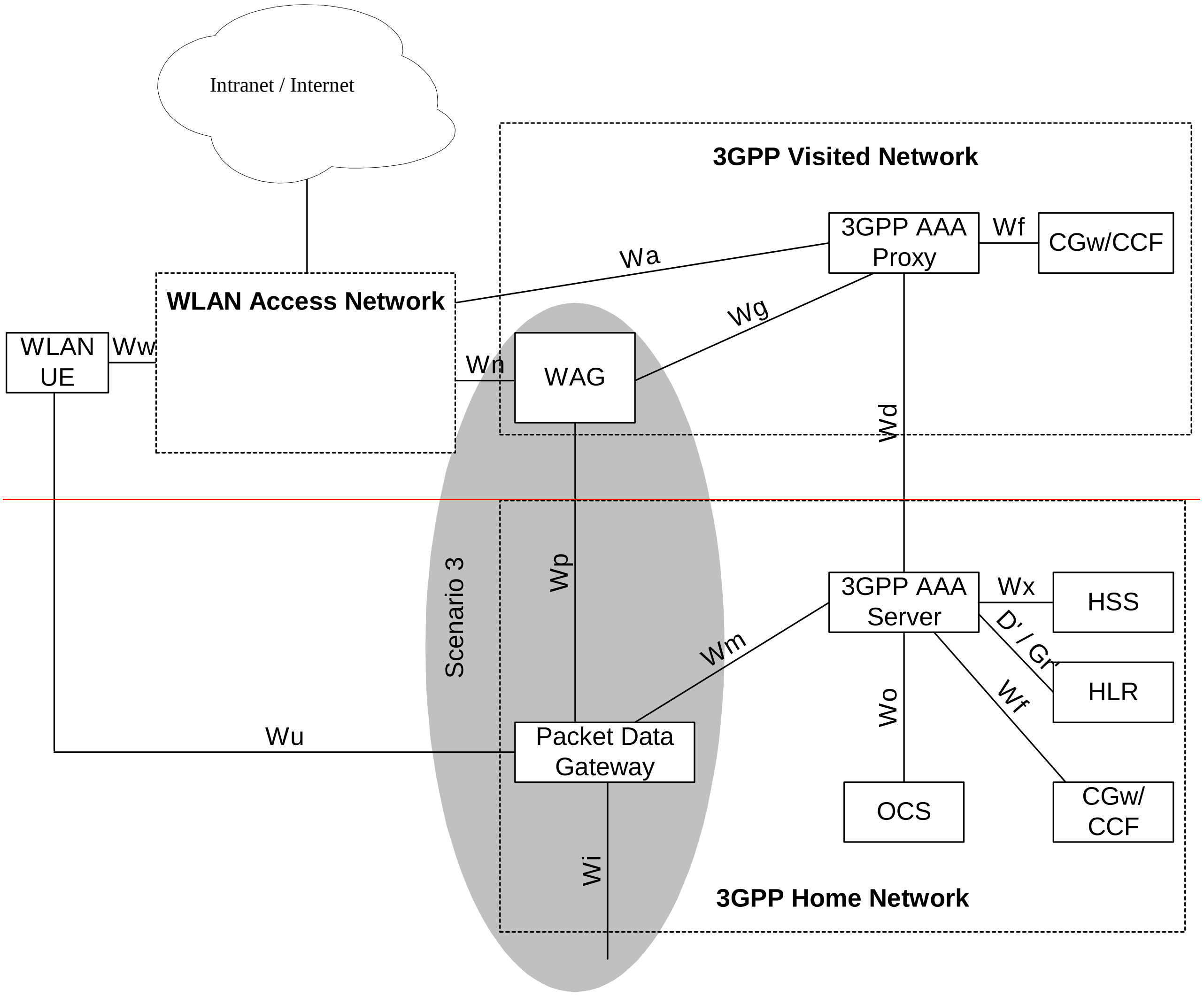
6.1.2 Roaming WLAN Inter-working Reference Model

The home network is responsible for access control. Charging records can be generated in the visited and/or the home 3GPP networks. The Wx and Wo reference points are intra-operator. The home 3GPP network interfaces to other 3GPP networks via the inter-operator Wd reference point.

The 3GPP AAA proxy relays access control signalling and accounting information to the home 3GPP AAA Server using the Wd reference point.

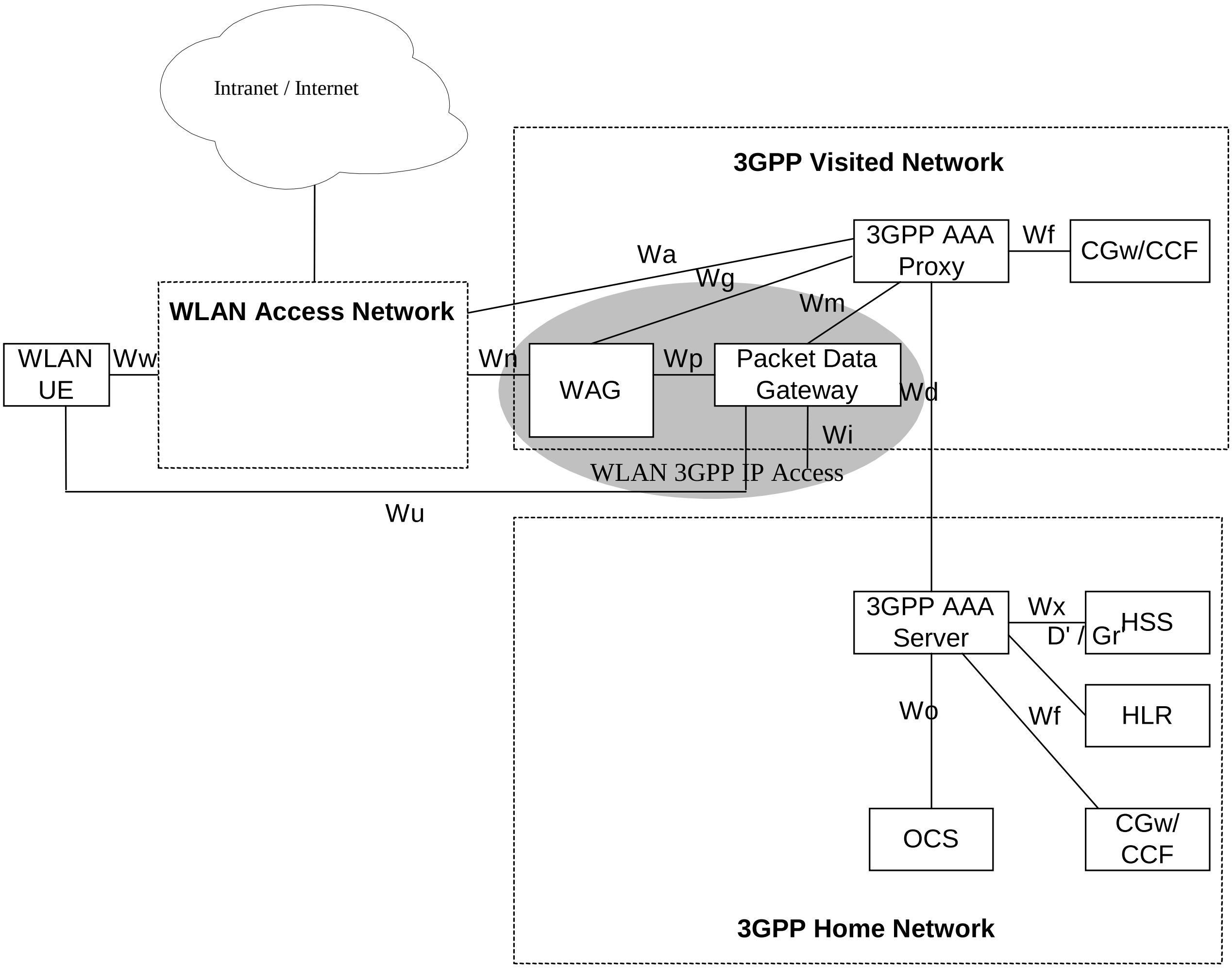
It can also issue charging records to the visited network CGw/CCF when required. The 3GPP network interfaces to WLAN Access Networks via the Wa reference point.

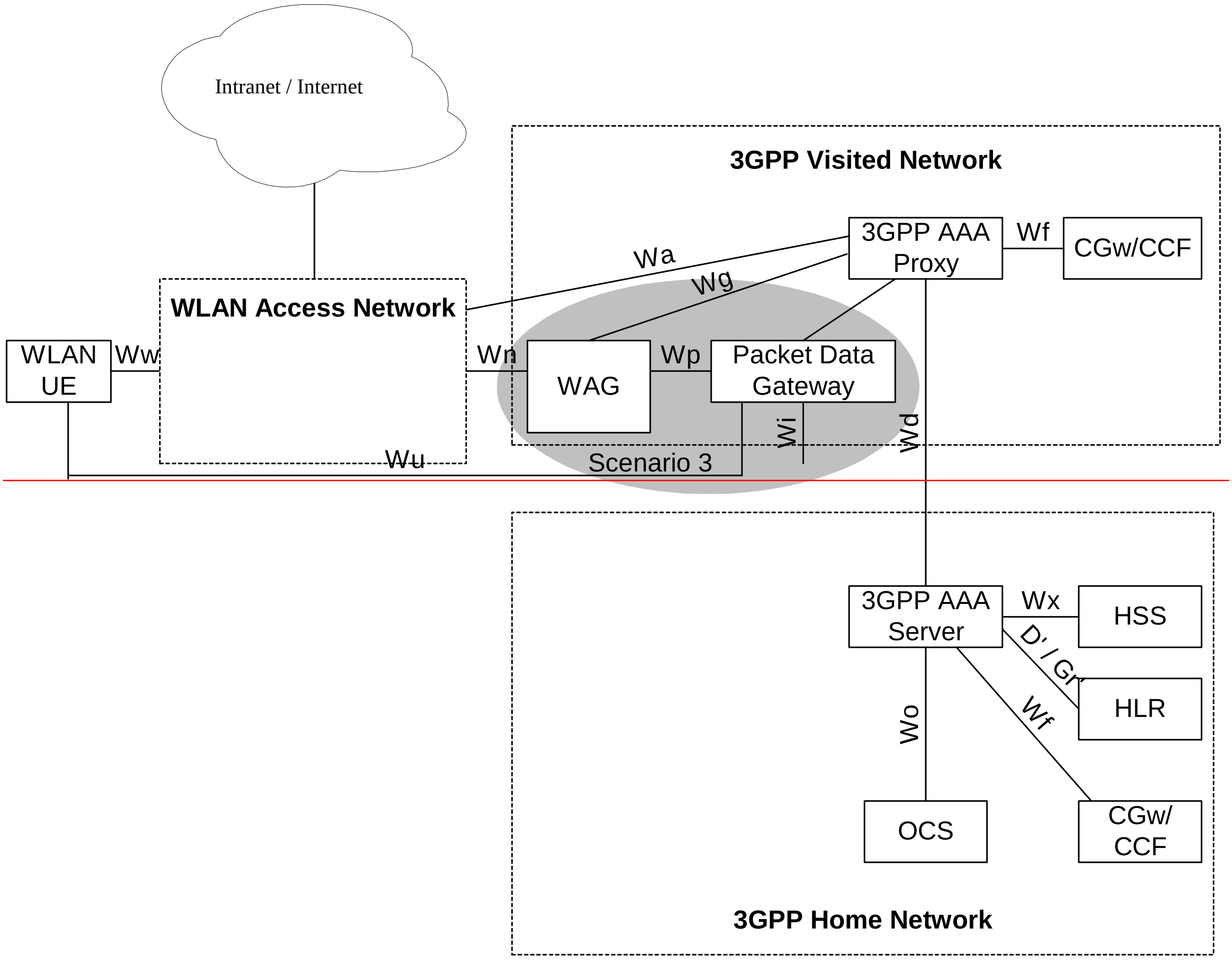

Intranet / Internet
3GPP Visited Network
3GPP AAA Proxy
Wf
CGw/CCF
Wa
Wg
WLAN Access Network
WLAN UE
Ww
Wn
WAG
Wd
WLAN 3GPP IP Access
Wp
3GPP AAA Server
Wx
D' / Gr
HSS
Wm
Wo
Wf
HLR
Wu
Packet Data Gateway
OCS
CGw/ CCF
Wi
3GPP Home Network



Note: The shaded area refers to WLAN 3GPP IP Access~~scenario 3~~ functionality.

Figure 6.2a: Roaming reference model - 3GPP PS based services provided via the 3GPP Home Network


Intranet / Internet
3GPP Visited Network
3GPP AAA Proxy
Wf
CGw/CCF
Wa
Wg
Wm
WLAN Access Network
WLAN UE
Ww
Wn
WAG
Wp
Packet Data Gateway
Wd
Wi
WLAN 3GPP IP Access
Wu
3GPP AAA Server
Wx
D' / Gr
HSS
Wo
Wf
HLR
OCS
CGw/ CCF
3GPP Home Network



Note: The shaded area refers to WLAN 3GPP IP Access ~~scenario 3~~ functionality.

Figure 6.2b.: Roaming reference model - 3GPP PS based services provided via the 3GPP Visited Network

6.2 Network elements

6.2.1 WLAN UE

A WLAN UE is the UE (equipped with UICC card including (U)SIM) utilized by a 3GPP subscriber to access the WLAN network for 3GPP interworking purpose. A WLAN UE may include terminal types whose configuration (e.g. interface to a UICC), operation and software environment are not under the exclusive control of the 3GPP system operator, such as a laptop computer or PDA with a WLAN card, UICC card reader and suitable software applications.

The WLAN UE functions include:

- Associating to an I-WLAN.
- WLAN access authentication based on EAP methods.
- Selection of a suitable VPLMN in the roaming case.
- Building an appropriate NAI.
- Obtain a local IP address.

For WLAN 3GPP IP Access enabled WLAN UE:

- Building an appropriate W-APN to be used ~~in ~~for External IP network selection~~scenario 3~~.
- Request the resolution of a W-APN ~~in scenario 3 ~~to a PDG address.
- Establish a secure tunnel~~ in scenario 3~~ to a PDG.
- Obtain a remote IP address~~ to be used in scenario 3~~.
- Accessing services provided in the operators PS domain.
- Allowing users to select the type of network access, i.e. ~~between direct access to external IP networks from the WLAN AN and network access through PLMN~~WLAN 3GPP IP Access or WLAN Direct IP Access.

6.2.1.1 WLAN UE classes

According to its capability, a WLAN UE is categorized into three classes.

Class WA WLAN UE: This class of a WLAN UE has both 3GPP and WLAN radio interfaces. The WLAN UE can be attached to both WLAN and 3GPP systems at the same time, when an interworking WLAN is available. Also it supports simultaneous access to both WLAN and 3GPP cellular network by activating both radio interfaces.

Class WB WLAN UE: This class of a WLAN UE has both 3GPP and WLAN radio interfaces. But it does not support simultaneous access to both WLAN and 3GPP cellular network because it can operate only one radio interface at a time.

Class WC WLAN UE: This class of a WLAN UE has only a WLAN radio interface. It is capable of WLAN attach and WLAN access only, when an interworking WLAN is available.

6.2.2 3GPP AAA Proxy

The 3GPP AAA Proxy represents a proxying and filtering function that –resides in the Visited 3GPP Network. The 3GPP AAA Proxy functions include:

- Relaying the AAA information between WLAN and the 3GPP AAA Server.
- Enforcing policies derived from roaming agreements between 3GPP operators and between WLAN operator and 3GPP operator
- Reporting per-user charging/accounting information to the VPLMN CCF/CGw for roaming users
- Service termination (O&M initiated termination from visited network operator)
- Protocol conversion when the Wa and Wd reference points do not use the same protocol

For WLAN 3GPP IP Access~~Scenario 3~~ only:

- Receiving authorization information related to subscriber requests for W-APNs in the Home or Visited network
- Authorization of access to Visited network W-APNs according to local policy

The 3GPP AAA Proxy functionality can reside in a separate physical network node, it may reside in the 3GPP AAA Server or any other physical network node.

6.2.3 3GPP AAA Server

The 3GPP AAA server is located within the 3GPP network. The 3GPP AAA Server:

- Retrieves authentication information and subscriber profile (including subscriber's authorization information) from the HLR/HSS of the 3GPP subscriber's home 3GPP network.
- Authenticates the 3GPP subscriber based on the authentication information retrieved from HLR/HSS. The authentication signaling may pass through AAA proxies.
- Communicates authorization information to the WLAN potentially via AAA proxies.

- Registers its (the 3GPP AAA server) address or name with the HLR/HSS for each authenticated and authorized 3GPP subscriber.
- Initiates the Purge procedure when the 3GPP AAA server deletes the information of a subscriber.
- May act also as a AAA proxy (see above).
- Maintains the WLAN UE's WLAN-attach status.
- Provides the WLAN UE's WLAN-attach status to other entities (which are out of the scope of this TS).
- Generates and reports per-user charging/accounting information to the HPLMN CCF/CGw.

For ~~scenario 3~~ WLAN 3GPP IP Access:

- Communicates service authorization information (e.g. authorized W-APN, necessary keying material for tunnel establishment and user data traffics) to the PDG. AAA proxies if the PDG is located in VPLMN.

********** MODIFIED SECTION **********

6.2.5 WLAN Access Gateway

The WLAN Access Gateway applies to a ~~scenario 3~~ WLAN 3GPP IP Access enabled system.

The WLAN Access Gateway is a gateway via which the data to/from the WLAN Access Network shall be routed via a PLMN to provide a WLAN UE with 3G PS based services in a ~~scenario 3~~ WLAN 3GPP IP Access enabled system.

The WLAN Access Gateway shall reside in the VPLMN in the roaming case, and in the HPLMN in the non-roaming case.

The WLAN Access Gateway:

- Allows VPLMN to generate charging information for users accessing via the WLAN AN in the roaming case.
- Enforces routing of packets through the PDG.
- Performs collection of per tunnel accounting information, e.g. volume count (byte count) and elapsed time, to be used for inter-operator settlements.
- Filters out packets based on unencrypted information in the packets. Packets should only be forwarded if they:

  1. are part of an existing tunnel or
  2. are expected messages from the WLAN UEs. This includes service requests, and tunnel establishment messages.

  Since the WAG does not have a full trust relationship with the WLAN UE, it is not able to stop all messages. However, messages from an unknown IP address can easily be discarded. Other approaches may be used as well. Additional types of message screening are left to the operators' control.

Note: per tunnel accounting generation in the WAG is not required when the WAG and PDG are in the same network, i.e. the non-roaming case.

The WAG shall implement policy enforcement.

If service is provided through a PDG in the HPLMN the WAG:

- Ensures that all packets from the WLAN UE are routed to the HPLMN.
- Ensures that packets from the authorised WLAN UEs are only routed to the appropriate PDG in the HPLMN and that packets from other sources than that PDG are not routed to the WLAN UE.

If service is provided through a PDG in the VPLMN the WAG:

- Ensures that all packets from the WLAN UE are routed to the VPLMN.
- Ensures that packets from the authorised WLAN UEs are only routed to the appropriate PDG in the VPLMN and that packets from other sources than that PDG are not routed to the WLAN UE.

6.2.5.1 Routing Enforcement

Information regarding the selected PDG, including whether the PDG is in the HPLMN or the VPLMN is provided by the HPLMN to the VPLMN.

In the roaming case, the PDG information is delivered from the 3GPP AAA Server to the 3GPP AAA Proxy.

Within the VPLMN, policy enforcement information is delivered to the WAG.

Note: Whether information regarding one or all PDGs is provided will likely impact the signalling which supports the activation of a further W-APN. Delivering information of all valid PDGs may limit impacts on signalling for further W-APN establishment.

The policy enforcement delivered during initial authentication will be bound to a user's AAA signalling. The WAG requires functionality to be able to securely bind this information to a user's traffic.

The binding of the policy to a user's traffic allows the WAG to drop un-authorized packets sent to/from a user.

6.2.5.2 Per-tunnel Charging Generation

Editor's Note: The details of per-tunnel charging generation in the WAG is FFS.

6.2.6 Packet Data Gateway

The Packet Data Gateway applies to a ~~scenario 3~~ WLAN 3GPP IP Access enabled system.

3GPP PS based services ~~(Scenario 3)~~ are accessed via a Packet Data Gateway. 3GPP PS based services may be accessed via a Packet Data Gateway in the user's Home Network or a PDG in the selected VPLMN. The process of authorisation and service selection (e.g. W-APN selection) and subscription checking determines whether a service shall be provided by the home network or by the visited network. The resolution of the IP address of the Packet Data Gateway providing access to the selected service will be performed in the PLMN functioning as the home network (in the VPLMN or HPLMN).

Successful activation of a selected service results in:

- Determination of the Packet Data Gateway IP address used by the WLAN UE;
- Allocation of a WLAN UE's remote IP address to the WLAN UE (if one is not already allocated);
- Registration of the WLAN UE's local IP address with the Packet Data Gateway and binding of this address with the WLAN UE's remote IP address.

The Packet Data Gateway:

- Contains routeing information for WLAN-3G connected users;
- Routes the packet data received from/sent to the PDN to/from the WLAN-3G connected user;
- Performs address translation and mapping;
- Performs de-capsulation and encapsulation;
- accepts or rejects the requested W-APN according to the decision made by the 3GPP AAA Server;
- redirects the tunnel establishment request towards another PDG if this is indicated to be done by the 3GPP AAA Server

Allows allocation of the WLAN UE's remote IP address;

- Relays the WLAN UE's remote IP address allocated by an external IP network to the WLAN UE, when external IP network address allocation is used.
- Performs registration of the WLAN UE's local IP address and binding of this address with the WLAN UE's remote IP address;
- Provides procedures for unbinding a WLAN UE's local IP address with the WLAN UE's remote IP address;
- Provides procedures for authentication and prevention of hijacking (i.e. ensuring the validity of the WLAN UE initiating any binding of the WLAN UE's local IP address with the WLAN UE's remote IP address, unbinding etc.)
- May filter out unauthorised or unsolicited traffic with packet filtering functions. All types of message screening are left to the operators' control, e.g. by use of Internet firewalls.
- Generates charging information related to user data traffic for offline and online charging purposes.
- May apply IP flow based bearer level charging [13], e.g. in order to differentiate or suppress WLAN bearer charging for 3GPP PS based services.
- Performs the functions of Service-based Local Policy Enforcement Point (controls the quality of service that is provided to a set of IP flow as defined by a packet classifier, control admission based on policy that is applied to the IP bearers associated with the flow, and configuration of the packet handling and "gating" functionality in the user plane.)
- Communicates with Policy Decision Function (PDF) to allow service-based local policy and QoS inter-working information to be "pushed" by the PDF or to be requested by the PDG. This communication also provides information to support the following functions in the PDG:
  - Control of Diffserv inter-working;
  - Control of RSVP admission control and inter-working;
  - Control of "gating" function in PDG;
  - WLAN bearer authorization;
  - QoS charging related function.

********** MODIFIED SECTION **********

6.3.6 Wg reference point

The Wg reference point applies to WLAN 3GPP IP Access ~~scenario 3~~.

This is an AAA interface between the 3GPP AAA Server/Proxy and the WAG. It is used to provide information needed by the WAG to perform policy enforcement functions for authorised users.

6.3.7 Wn reference point

The Wn reference point applies to ~~scenario 3~~ WLAN 3GPP IP Access.

This is the reference point between the WLAN Access Network and the WAG. This interface is to force traffic on a WLAN UE initiated tunnel to travel via the WAG. There can be several different ways to implement this interface as shown in Annex C. The specific method to implement this interface is subject to local agreement between the WLAN AN and the PLMN.

6.3.8 Wp reference point

The Wp reference point applies to ~~scenario 3~~ WLAN 3GPP IP Access.

This is the reference point between the WAG and PDG.

6.3.9 Wi reference point

The Wi reference point applies to ~~scenario 3~~ WLAN 3GPP IP Access.

This is the reference point between the Packet Data Gateway and a packet data network. The packet data network may be an operator external public or private packet data network or an intra operator packet data network, e.g. the entry point of IMS, RADIUS Accounting or Authentication, DHCP.

Wi reference point is similar to the *Gi* reference point provided by the PS domain. Interworking with packet data networks is provided via the Wi reference point based on IP. Mobile terminals offered services via the Wi reference point may be globally addressable through the operators public addressing scheme or through the use of a private addressing scheme.

6.3.10 Wm reference point

The Wm reference point applies to WLAN 3GPP IP Access~~scenario 3~~.

This reference point is located between 3GPP AAA Server and Packet Data Gateway respectively between 3GPP AAA Proxy and Packet Data Gateway. The functionality of this reference point is to enable:

- The 3GPP AAA Server/Proxy to retrieve tunneling attributes and WLAN UE's IP configuration parameters from/via Packet Data Gateway.
- Carrying messages for service authentication between WLAN UE and 3GPP AAA server/proxy.
- Carrying messages for service authorization between PDG and 3GPP AAA server/proxy.
- Carrying authentication data for the purpose of tunnel establishment, tunnel data authentication and encryption.

********** MODIFIED SECTION **********

6.3.12 Wu reference point

The Wu reference point applies to ~~scenario 3~~WLAN 3GPP IP Access.

The Wu reference point is located between the WLAN UE and the Packet Data Gateway. It represents the WLAN UE-initiated tunnel between the WLAN UE and the Packet Data Gateway. Transport for the Wu reference point protocol is provided by the Wn and Wp reference points, which ensure that the data are routed via the WLAN Access Gateway where routing enforcement is applied.

The functionality of the Wu reference point is to enable:

- WLAN UE-initiated tunnel establishment
- User data packet transmission within the WLAN UE-initiated tunnel
- Tear down of the WLAN UE initiated tunnel

********** MODIFIED SECTION **********

7.3.1 Access and service Authorization information update procedure

This procedure is for WLAN 3GPP ~~senario3.~~IP Access.

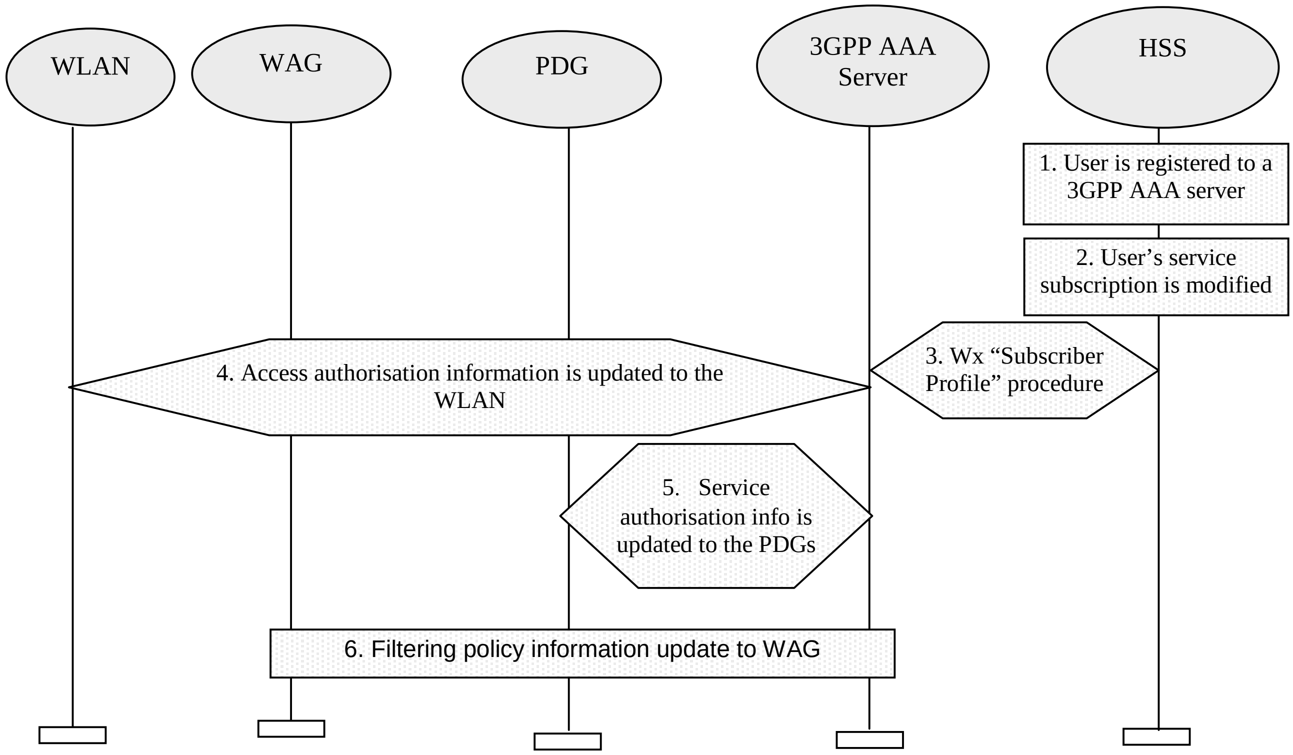

WLAN
WAG
PDG
3GPP AAA Server
HSS
1. User is registered to a 3GPP AAA server
2. User's service subscription is modified
3. Wx "Subscriber Profile" procedure
4. Access authorisation information is updated to the WLAN
5. Service authorisation info is updated to the PDGs
6. Filtering policy information update to WAG

Figure 7.4: Authorization information Update Procedure

1. User is registered to a 3GPP AAA server
2. User's service subscription is modified in the HSS e.g. via O&M,
3. HSS updates the profile information stored in the registered 3GPP AAA server by Wx reference point procedure "Subscriber Profile".
4. The WLAN access authorisation information of the associated connection is updated to WLAN if necessary.
5. The service authorisation information of the activated services is updated to PDGs if necessary. A deactivation of service may be initiated if the subscriber lost the authorization of the activated service.
6. The filtering policy information of the activated services is updated to WAG if necessary.

Note: The de-registration may be initiated by the AAA server to the HSS as necessary, i.e., the AAA server determines that the WLAN UE is unable to access any service upon the updated authorization.

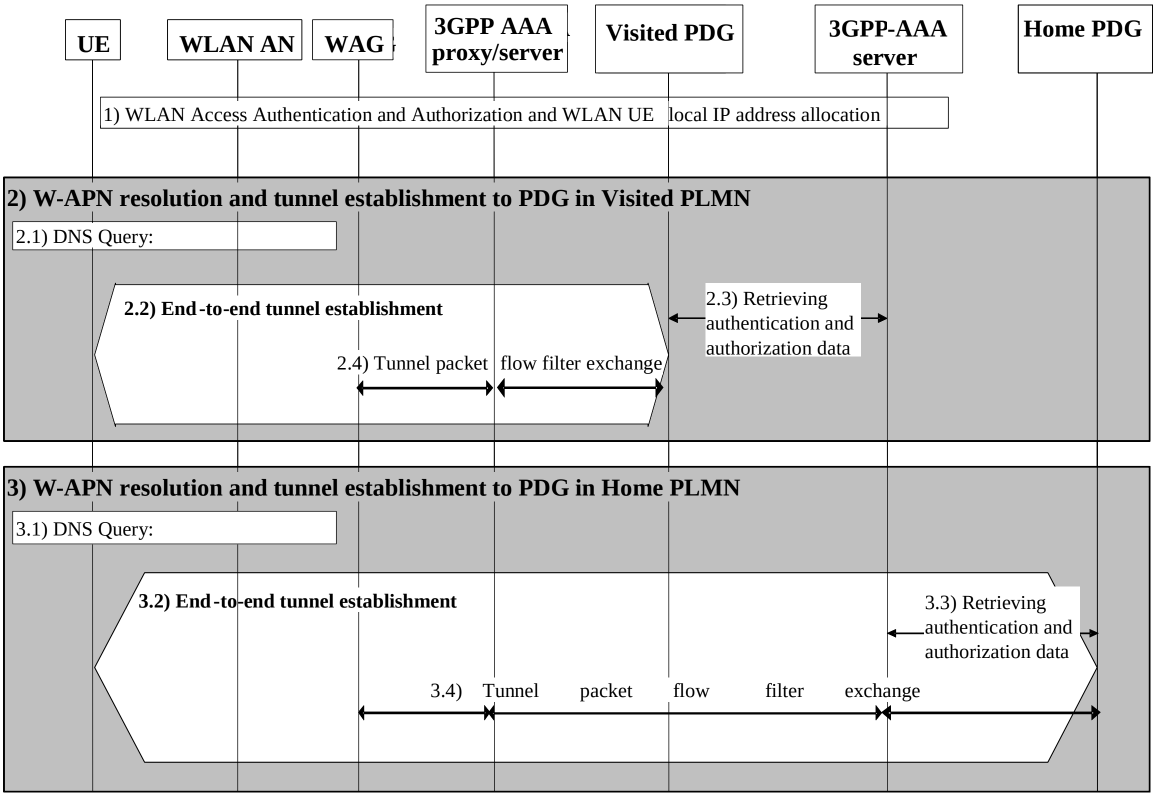
********** MODIFIED SECTION **********

7.9 W-APN resolution and Tunnel establishment

This information flow presents the generic message exchange necessary in order to resolve the selected W-APN and establish a WLAN UE-Initiated tunnel for ~~Scenario 3~~WLAN 3GPP IP Access purposes.

As a prerequisite of these procedures it is necessary to perform the following:

1. WLAN Access Authentication and Authorisation and provisioning of the WLAN UE's local IP address



UE
WLAN AN
WAG
3GPP AAA proxy/server
Visited PDG
3GPP-AAA server
Home PDG
1) WLAN Access Authentication and Authorization and WLAN UE local IP address allocation
2) W-APN resolution and tunnel establishment to PDG in Visited PLMN
2.1) DNS Query:
2.2) End-to-end tunnel establishment
2.3) Retrieving authentication and authorization data
2.4) Tunnel packet flow filter exchange
3) W-APN resolution and tunnel establishment to PDG in Home PLMN
3.1) DNS Query:
3.2) End-to-end tunnel establishment
3.3) Retrieving authentication and authorization data
3.4) Tunnel packet flow filter exchange

Figure 7.10: Example message flow to WLAN UE-Initiated tunnel establishment

When the user decides that he wants to access a service, the WLAN UE selects the W-APN network ID associated to the service requested by the user.

A detailed description of the W-APN resolution and the WLAN UE-Initiated Tunnel Establishment is given below.

2. Depending on internal configuration, the WLAN UE initiates W-APN resolution and tunnel establishment with a PDG in VPLMN.

Note: The configuration of the WLAN UE regarding W-APNs can be controlled by e.g. USIM Application Toolkit-based mechanisms.

2.1 UE constructs an FQDN using the W-APN Network Identifier and VPLMN ID as the Operator Identifier and performs a DNS query to resolve it. The DNS response will contain one or more IP addresses of equivalent PDGs that support the requested W-APN in the VPLMN according to standard DNS procedures.
If the VPLMN does not support the W-APN, then the DNS query returns a negative response. In this case, the WLAN UE continues with step 3.

2.2 The WLAN UE selects a PDG from the list received in step 2.1, and the establishment of an end-to-end tunnel is performed between the WLAN UE and this PDGs. The WLAN UE shall include the W-APN and the user identity in the initial tunnel establishment request.

2.3 During the tunnel establishment, the PDG contacts the 3GPP AAA Server in the HPLMN via the 3GPP AAA proxy for authorization of the WLAN UE and to retrieve the information required for the mutual authentication part of the tunnel establishment.
The 3GPP AAA Server verifies that the user requesting the tunnel establishment has been already successfully WLAN Access Authorized. If not, the tunnel establishment request is rejected.
If the WLAN UE is not allowed to use a visited-PDG to access the given W-APN, then the tunnel establishment shall be rejected by the PDG.

If it is not possible to establish the tunnel with any of the PDG ~~recieved~~received from step2.1, or the tunnel establishment failure reason is that the WLAN UE is not allowed to use a visited-PDG to access the given W-APN, then the WLAN UE continues with step 3.

2.4 During the tunnel establishment procedure, the PDG and the WAG exchange information via the 3GPP AAA Proxy in order to establish a filtering policy to allow the forwarding of tunnelled packets to the PDG. The 3GPP AAA Proxy requests the WAG to apply filtering policy based on information obtained from the PDG. The 3GPP AAA Proxy decides which filtering policy could be applied by the WAG according to local information (e.g. based on number of users, WAG capabilities, roaming agreement policy, etc).

3. Depending on internal configuration, or due to the failure of step 2.1 or 2.3, the WLAN UE initiates W-APN resolution and tunnel establishment with a PDG in HPLMN.

3.1 UE constructs an FQDN using W-APN Network Identifier and the HPLMN ID as the Operator Identifier, and performs a DNS query to resolve it. The DNS response will contain one or more IP addresses of equivalent PDGs that support the requested W-APN in the HPLMN according to standard DNS procedures.

3.2 The WLAN UE selects a PDG from the list received in step 3.1, and the establishment of an end-to-end tunnel is performed between the WLAN UE and this PDGs. The WLAN UE shall include the W-APN and the user identity in the initial tunnel establishment request.

3.3 During the tunnel establishment, the PDG contacts the 3GPP AAA Server in the HPLMN for authorization of the WLAN UE and to retrieve the information required for the mutual authentication part of tunnel establishment. The 3GPP AAA Server verifies that the user requesting the tunnel establishment has been already WLAN Access Authorized. If not, the tunnel establishment request is rejected.
If the WLAN UE is not allowed to use a Home PDG to access the given W-APN according to his subscription, then the tunnel establishment shall be rejected by the Home PDG.

3.4 During the tunnel establishment, the PDG and the WAG exchange information via the 3GPP AAA Server and 3GPP AAA Proxy in order to establish a filtering policy to allow the forwarding of tunnelled packets to the PDG. The 3GPP AAA server requests to the WAG to apply filtering policy based on information obtained from the PDG. The 3GPP AAA server decides which filtering policy could be applied by the WAG according to local information (e.g. based on number of user, WAG capabilities, roaming agreement policy, etc). The applied filtering policy is communicated to the Home-PDG.

7.9.1 Redirection

In the above procedures, the WLAN UE may not be authorised to access the requested W-APN through the selected PDG. This may occur for the following reasons:

(i) The requested W-APN is not supported by the network

(ii) The user is not subscribed to the requested W-APN

(iii) The PDG is in the VPLMN and the user's subscription indicates that VPLMN access is not allowed for the requested W-APN

(iv) The operator does not wish to include all PDG addresses in DNS and so (for example) all initial requests are handled by a default PDG which may not be the correct PDG for the requested W-APN

(v) The user has not supplied an explicit requested W-APN. This is treated as a request for the first appropriate subscribed W-APN, or for a network default W-APN (if a wildcard W-APN is included in the subscription), as per 23.060 Annex A.

In cases (i), (ii) and (iii), the request is simply rejected. In case (iii), the WLAN UE may attempt tunnel establishment to the HPLMN as described in Section 7.8.

In cases (iv) and (v) above, the AAA Server may determine that the user is authorised to access the W-APN through a different PDG. The IP address of the alternative PDG is then returned to the WLAN UE in the rejection message from PDG to WLAN UE. In this case the WLAN UE shall attempt a new tunnel establishment request to the provided PDG address.

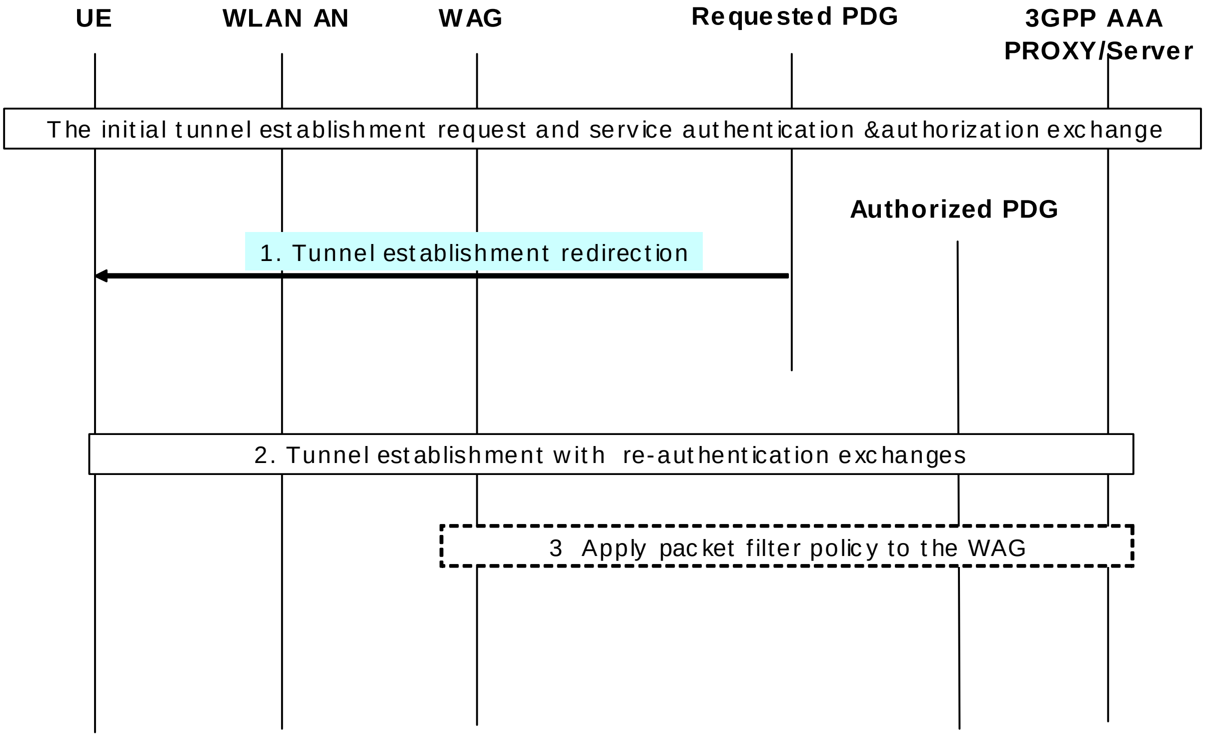

UE
WLAN AN
WAG
Requested PDG
3GPP AAA PROXY/Server
The initial tunnel establishment request and service authentication &authorization exchange
Authorized PDG
1. Tunnel establishment redirection
2. Tunnel establishment with re-authentication exchanges
3 Apply packet filter policy to the WAG

Figure 7.11: Message flow of the tunnel establishment with redirection

During the step 2.3/3.3 in the procedure of clause 7.9, the 3GPP AAA Server authorizes the service to the WLAN UE, and sends the authorization information to the requested PDG. If requested PDG is not authorized to provide the service then the AAA server sends a new PDG (Authorized PDG) address and the authorized W-APN, then the following steps performed:

1. The requested PDG sends tunnel redirection request to the UE with service authorization information (authorized PDG address, authorized W-APN and the re-authentication parameters provided by the AAA server).

2. The WLAN UE sends an end-to-end tunnel establishment request to the Authorized PDG. Then end-to-end tunnel establishment begins between the Authorized PDG and the WLAN UE. A re-authentication method should be used during this tunnel establishment.

3. The Authorized PDG provides filtering information to the WAG as it is specified in clause 7.9.

7.9.2 Subsequent authentication

In the case that the user attempts a subsequent tunnel establishment to a different PDG, it should be possible to avoid repeating the full authentication process (for example, a shorter re-authentication process should be used). This is ffs in Stage 3 work.

7.9.3 Use of DNS

It shall be possible to restrict the propagation of DNS information used for the above mechanism to DNS servers controlled by the PLMNs and to DNS servers available only to authorised 3GPP WLAN UEs (i.e. those WLAN UEs which have successfully connected to a 3GPP Interworking WLAN.)

It shall be possible to configure multiple PDG addresses against a single FQDN in a manner which allows the load to be shared across these PDGs.

Note: The above shall be achieved by standard DNS mechanisms. The usage of TLD and the DNS query performed by the WLAN UE to resolve the W-APN are left to stage 3. Further details are in [5]**.**

7.9.4 Subsequent tunnel establishment

The subsequent tunnel establishment should follow the same procedure as in the first tunnel establishment.

********** MODIFIED SECTION **********

C.1 WLAN shared by (or connected to) multiple ISPs and PLMNs

This is typically when a WLAN AN is owned by an independent entity such as a hotel and the owner allows subscribers of ISPs to use their WLAN AN by using the ISP network. However, WLAN AN owned by an ISP or a PLMN may also allow other ISP/PLMN subscribers to use the WLAN in a similar way.

In this situation, the WLAN AN may be connected to multiple ISPs and PLMNs in the layer 2 for ~~scenario 3~~WLAN 3GPP IP Access as shown in Figure C.1.1. Another solution using DNS and NAT is described in C.2.3.

To this end, VLAN or other layer 2 tunnelling capabilities may be implemented in APs or access controller in WLAN AN in order to separate traffic of different networks.

The interface between the WLAN AN and the PLMN may be a Layer 2 tunnel, such as VLAN, Martini, or VPLS, etc. The WAG takes the role of the access router of the WLAN AN. This enables end to end tunnelling for ~~scenario 3~~WLAN 3GPP IP Access, even when the IP address of the PDG is not routable on the Internet.

The local IP address of a WLAN UE, when using ~~in scenario 3~~WLAN 3GPP IP Access, belongs to the PLMN's IP address space. So, all the packets to a WLAN UE shall pass through the PLMN.

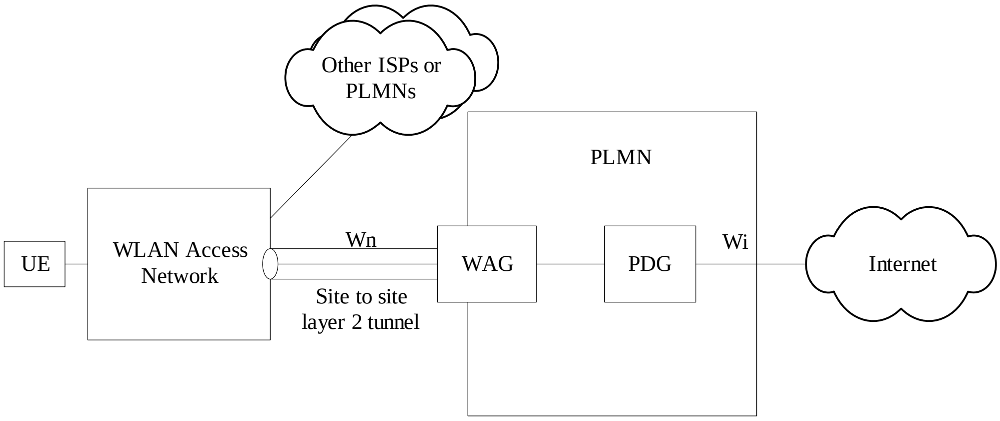


Figure C.1.1: Wn Interface when WLAN is connected to multiple ISPs and PLMNs

********** MODIFIED SECTION **********

C.2.3 Separating traffic to different VPLMNs using a combined DNS/NAT approach

If the WLAN UE is associated to the WLAN AN and authenticated through EAP, it can access the Internet directly (for WLAN Direct IP Access~~scenario 2~~) or establish a tunnel to a PDG in the VPLMN/HPLMN to access 3GPP PS based services (~~scenario 3~~for WLAN 3GPP IP Access). Both ~~scenarios~~ cases must be enabled in parallel. The WLAN UE performs a DNS query to resolve a W-APN to a PDG address. This IP address is the tunnel endpoint in the PLMN. If the PDG resides in the HPLMN, it must be possible to route traffic to the PDG through the selected VPLMN. The combined DNS/NAT approach as described in this chapter adds no requirements to the WLAN UE and HPLMN and uses only normal IP routing capabilities in the VPLMN.

The main idea is to use some kind of "reverse NAT" in the VPLMN that maps the PDG address received in the answer to the WLAN UE's DNS request to an address out of the address range of the VPLMN. Each PDG address is mapped to one VPLMN address, which may be a private address, depending on the addresses used in the WLAN AN. For simplicity (no new protocol needed) and performance reasons the VPLMN DNS proxy and the desired reverse NAT function are implemented on the WAG. Thus, inside of the NAT is the HPLMN address space, outside is the WLAN AN address space.

As the WLAN is directly connected to the VPLMN it is aware about the VPLMN IP addresses and can easily route ~~scenario 3~~WLAN 3GPP IP Access traffic to the correct VPLMN. The VPLMN maps the destination address of the IP packet to the stored PDG address and forwards the packet to the HPLMN. WLAN Direct IP Access~~Scenario 2~~ traffic goes to the default route configured in the WLAN edge router, i.e. to the Internet.

The following figure shows the process of W-APN resolution and NAT in the VPLMN. The figure shows a local DNS server in the WLAN AN while it is also possible that the WLAN UE receives the address of a DNS server in the VPLMN by DHCP or during EAP authentication. If the WLAN UE wants to access a PDG in the HPLMN, the W-APN indicates the HPLMN and optionally the VPLMN, otherwise the W-APN indicates the VPLMN only.

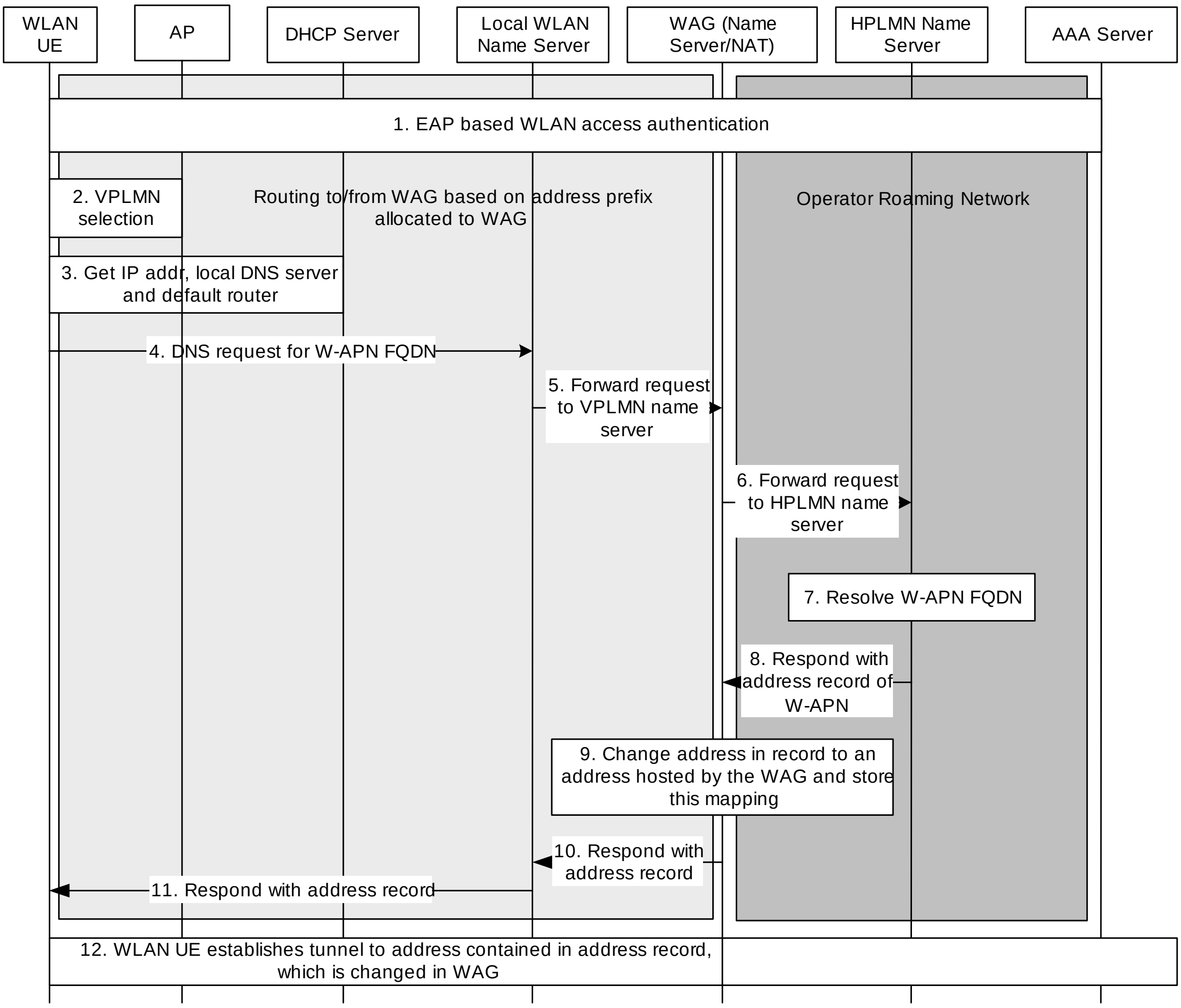

WLAN UE
AP
DHCP Server
Local WLAN Name Server
WAG (Name Server/NAT)
HPLMN Name Server
AAA Server
1. EAP based WLAN access authentication
2. VPLMN selection
Routing to/from WAG based on address prefix allocated to WAG
Operator Roaming Network
3. Get IP addr, local DNS server and default router
4. DNS request for W-APN FQDN
5. Forward request to VPLMN name server
6. Forward request to HPLMN name server
7. Resolve W-APN FQDN
8. Respond with address record of W-APN
9. Change address in record to an address hosted by the WAG and store this mapping
10. Respond with address record
11. Respond with address record
12. WLAN UE establishes tunnel to address contained in address record, which is changed in WAG

Figure C.2.2: DNS controlled reverse NAT procedure

1. WLAN access authentication procedure between WLAN UE and AAA server based on EAP.
2. WLAN UE retrieves PLMN list from WLAN and selects a preferred VPLMN.
3. WLAN UE gets transport IP address, local name server (optionally) and default router address via DHCP.
4. WLAN UE builds W-APN FQDN indicating VPLMN (optionally) and HPLMN and sends DNS request to local name server or directly to the name server in the VPLMN.
5. Local name server inspects W-APN FQDN and forwards DNS request to VPLMN name server. VPLMN name server is implemented together with a "reverse" NAT and probably a Firewall on the WAG.
6. VPLMN name server inspects W-APN FQDN and forwards DNS request to HPLMN name server through GPRS roaming network.
7. HPLMN name server resolves W-APN.
8. HPLMN name server responds to VPLMN name server with an address record of the W-APN.
9. VPLMN name server (acting as DNS Proxy) optionally changes the PDG address contained in the address record to an address of the WAG address space (this address may be a private address) and stores the mapping between the two addresses. The new address must be routable within the WLAN to the WAG. Changing the addressses may be an option configurable by the operator.
10. VPLMN name server responds the address record to local name server.
11. Local name server responds the address record to WLAN UE.

12. WLAN UE establishes tunnel to the address contained in the address record. This may be an address hosted by the WAG (otherwise it is the PDG address). This address is changed ("NATted") at the WAG to the "real" PDG address.

C.3 WLAN AN exclusively owned by and connected to a single PLMN

This is when a PLMN operator installs its own WLAN AN without any connections to other ISPs or PLMNs.

In this case, WLAN AN can be regarded as an extension of the PLMN's IP network and no tunnel is required between WLAN AN and PLMN. The local IP address of a WLAN UE in ~~scenario 3~~WLAN 3GPP IP Access belongs to the PLMN's IP address space.

C.4 WLAN AN connected to a single ISP

This is when WLAN AN is solely connected to an ISP's backbone network. WLAN AN is regarded as an extension of the ISP's backbone network. Many legacy WLAN ANs can be categorized to this case

The connectivity between the WLAN AN and the PLMN is in layer 3 through the ISP's backbone network as shown in Figure C.4.1.

This kind of WLAN AN supports ~~scenario 2~~WLAN Direct IP Access as defined in the TS 23.234, i.e. the authenticated WLAN UE can access the Internet directly via the ISP.

For ~~scenario 3~~WLAN 3GPP IP Access, the local IP address of a WLAN UE is generally allocated by the ISP and it belongs to the ISP's IP address space. When PLMN allocates WLAN UE's local IP address, a layer 2 tunnel is required.

When the end to end tunnelling is used between a WLAN UE and a PDG and the IP address of the PDG is non-routable in the Internet, an additional means is required for routing the packets to the PDG and to meet the routing enforcement requirement.

It is FFS for methods to enable WLAN 3GPP IP Access~~scenario 3~~ for this kind of WLAN AN.

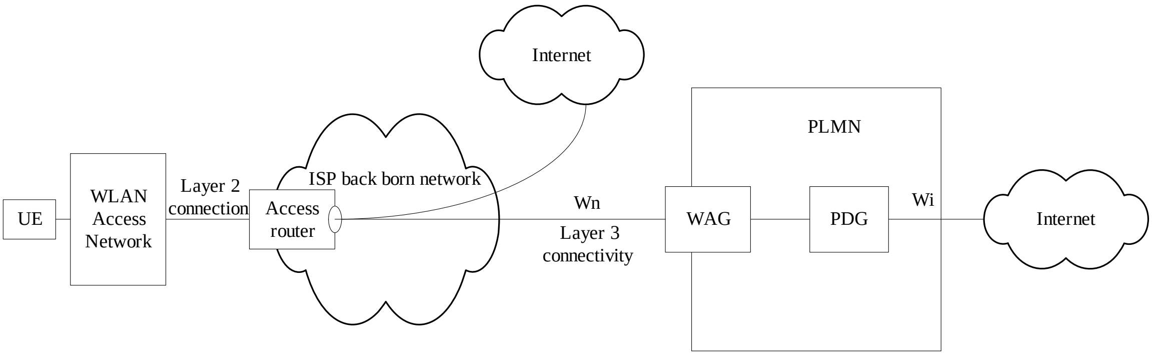


Figure C.4.1: Wn Interface when WLAN is connected to a PLMN through an ISP

********** MODIFIED SECTION **********

E.3 WAG Description

Support of the WAG for ~~in~~ ~~scenario 3~~WLAN 3GPP IP Access is mandatory for both roaming and non-roaming cases.

The WAG shall:

- Support the setup of a secure tunnel initiated by the WLAN UE, and cooperate with the PDG to supply required parameters (e.g. DNS address, DHCP address, etc) from the destination network to the WLAN UE.

- Resolve the address of the PDG from the W-APN information supplied by the WLAN UE and verified with the 3G AAA Server.

- Set up a tunnel to the appropriate PDG(s).

- Route packets between the WLAN UE initiated tunnel and the tunnel to the PDG.

- Serve as a firewall for the network connecting the WAG and PDG, allowing only trusted packets into the 3G network.

- Update user status information in the 3G AAA Server.

- Generate accounting information, especially when located in the VPLMN.

E.4 Wu Reference Point

The reference point Wu is located between the WLAN UE and the WAG. The purpose of this reference point is to transport tunnelled user data traffic securely between the WLAN UE and the 3GPP network to provide PS-based services to the WLAN UE. In roaming cases, the Wu reference point is terminated between the WLAN UE and the WAG in the VPLMN. The WLAN may apply a routing enforcement policy, if necessary, to ensure packets are routed only to the WAG.

This reference point is not required to be used when no 3G PS-based Services are provided and a direct connection to external IP network (Internet/Intranet) exists in which case the user data can be directly routed from the WLAN access network without passing 3GPP network, as it is the ~~case with scenario 2~~WLAN Direct IP Access.

No specific tunnelling protocol is specified for the Wu reference point, but the current working assumption is that the WLAN UE will be able to use an existing VPN client.

3GPP TSG-SA WG2 #40
Sophia Antipolis, France, 17th – 21st May 2004

Tdoc ⌘S2-042320

revised s2-042220, s2-041849, s2-041807

CR-Form-v7

CHANGE REQUEST

⌘	**23.234**	**CR**	**033**	⌘**rev**	**3**	⌘	Current version:	**6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME □ Radio Access Network □ Core Network ☒

Title:	⌘	WLAN UE initiated disconnection procedure		
Source:	⌘	SA2 (Huawei, ChinaMoble)		
Work item code:	⌘	WLAN	***Date:*** ⌘	21/05/2004
Category:	⌘	**F**	***Release:*** ⌘	Rel-6
		Use one of the following categories: ***F*** *(correction)* ***A*** *(corresponds to a correction in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)* Detailed explanations of the above categories can be found in 3GPP TR 21.900.	*Use one of the following releases:* *2 (GSM Phase 2)* *R96 (Release 1996)* *R97 (Release 1997)* *R98 (Release 1998)* *R99 (Release 1999)* *Rel-4 (Release 4)* *Rel-5 (Release 5)* *Rel-6 (Release 6)*	

Reason for change:	⌘	In the TS 23.234 v6.0.0, no Procedure or description addresses the UE initiated disconnection, a important basic procedure for other fundamental features...
Summary of change:	⌘	The description of the principles and main points of WLAN UE initiated disconnection procedure is introduced
Consequences if not approved:	⌘	An important feature as preconditions for main procedures leaves unclear in the current TS.

Clauses affected:	⌘	7				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

******************New Text For the TS****************

7.X The WLAN UE initiated WLAN AN Access disconnection

The WLAN UE may disconnect the from WLAN AN by:

- initiating a disconnection of the WLAN radio connection;
- initiating a disconnection of the WLAN IP connectivity.

Disconnection of the WLAN radio connection

Upon receiving a WLAN radio disconnection request (e.g., Disassociation in case of IEEE802.11 WLAN AN) from the WLAN UE with the WLAN access connection, the WLAN AN should perform the "disconnecting a subscriber by WLAN AN" (section 7.5) during or after the WLAN radio disconnection, with or without confirm message to the WLAN UE.

Disconnection of the WLAN IP connectivity

The UE initiated disconnection of the WLAN IP connectivity is usually performed before the disconnection of the WLAN radio connection and after the disconnection of the 3GPP PS access tunnels. However the WLAN UE may initiate a WLAN IP connectivity disconnection before the 3GPP PS access tunnels are disconnected. This will trigger the tunnel disconnection procedure specified in section 7.10.2.

If the WLAN UE initiates a disconnection of the WLAN IP connectivity:

1. The WLAN UE may initiate a disassociation after the disconnection procedure.

2. The WLAN AN stops the connection under ther request of the WLAN UE, e.g. close the opened port to the WLAN UE.

3. The WLAN AN should perform the "disconnecting a subscriber by WLAN AN" during or after the disconnection of WLAN access connection.

The WLAN AN should initiate an authentication or a disconnection of WLAN radio connection with this WLAN UE, if the WLAN UE keeps the WLAN radio connection without subsequent indication or requests in a certain period of time.

The 3GPP PS Access tunnel disconnection

The UE initiated tunnel disconnection is usually performed before the disconnection of WLAN IP connectivity and the disconnection of the WLAN radio connection. However, the WLAN UE may directly initiate a disconnection of the WLAN radio connection as a fast disconnection option when tunnel connections with PDG exist. This will trigger the tunnel disconnection procedure specified in section 7.10.2.

3GPP TSG-SA WG2 #40 ***Tdoc ⌘S2-042226***
Sophia Antipolis, France, 17th – 21st May 2004

revised s2-041839,1810, combined S2-041651

CR-Form-v7

CHANGE REQUEST

⌘	**23.234**	**CR**	**035**	⌘**rev**	**2**	⌘	Current version:	**6.0.0**	⌘	

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: WLAN access □ ME □ Radio Access Network □ Core Network ☒

Title:	⌘	**Clarification on policy enforcement and WLAN access authentication & authorisation**		
Source:	⌘	SA2 (China Mobile,Huawei, Siemens, Nortel, Samsung)		
Work item code:	⌘	WLAN	***Date:*** ⌘	19/05/2004
Category:	⌘	**F** *Use one of the following categories:* ***F*** *(correction)* ***A*** *(corresponds to a correction in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)* Detailed explanations of the above categories can be found in 3GPP TR 21.900.	***Release:*** ⌘	Rel-6 *Use one of the following releases:* *2 (GSM Phase 2)* *R96 (Release 1996)* *R97 (Release 1997)* *R98 (Release 1998)* *R99 (Release 1999)* *Rel-4 (Release 4)* *Rel-5 (Release 5)* *Rel-6 (Release 6)*

Reason for change:	⌘	In the previous meeting, it was concluded the policy enforcement in the WAG before tunnel establishment is ffs. It is a consensus of most operators that some rule/policy information is necessary to be sent to WAG from 3GPP AAA server during the course of WLAN access authentication/authorisation procedure; this can help the PLMN prevent the unwanted packets as much as possible, as earlier as possible. Although the WLAN AN can help with this, it is concluded that the PLMN still need necessary firewall policy to prevent unwanted packets whenever possible, it should not depend only on WLAN AN for this. For operators hope to prevent the unwanted packets out of their PLMN in earlier stage, they can arrange the network to enable the WAG to bind the policy information to a user's traffic. For example, to allocate the transport IP in the VPLMN. So it is necessary to clarify the fact of this issue: it is feasible to be deployed with proper network arrangment, and the related procedure should be corrected and completed in the TS.
Summary of change:	⌘	Add the clarification of the policy enforcement in the WAG before tunnel establishmen in clause 6.2.5, 6.2.5.1. Change the procedure in clause 7.2 by adding process for policy enforcement information delivery between AAA Server and WAG before tunnel establishment as an optional step. The CR028rev3(S2-041651) approved in SA2#39 is combined
Consequences if not approved:	⌘	The WLAN authentication/authorization procedure is not complete, the policy enforcement in the WAG before tunnel establishment is still ffs.

Clauses affected:	⌘	3.1, 6.2.5, 6.2.5.1,7.2				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

********** MODIFIED SECTION **********

3.1 Definitions

Available SSID: It is an SSID that the WLAN UE has found after active and/or passive scanning which meets certain conditions as specified in IEEE 802.11 [19].

3GPP - WLAN Interworking: Used generically to refer to interworking between the 3GPP system and the WLAN family of standards**.** Annex B includes examples of WLAN Radio Network Technologies.

Environment: The type of area to be covered by the WLAN network of a 3GPP - WLAN interworking; e.g. public, corporate and residential.

External IP Network/External Packet Data Network: An IP network to which access may be provided through the 3GPP system, rather than directly from the WLAN AN. For example, the Internet, an operator's IP network or a 3rd party IP network such as a corporate IP network.

Home WLAN: The WLAN that is interworking with the HPLMN of the 3GPP - WLAN interworking user.

Interworking WLAN : WLAN that interworks with a 3GPP system**.**

I-WLAN selection: Procedure for the selection among the available I-WLAN APs

Offline charging: Offline charging mechanism is provided for collecting and forwarding charging information about occurred WLAN access resource and core network resource usage, etc without affecting the service rendered in real-time.

Online charging: Online charging mechanism is provided where the service rendered is affected in real-time and is required for a direct interaction with session/service control. This allows an online charged subscriber to access WLAN.

Policy Enforcement: In scenario 3, Policy Enforcement is implemented in a WAG. ~~to allow only authorized packets to/from a WLAN AN to pass through.~~Packets coming from or going to the WLAN AN are policed based on unencrypted data within the packets. (e.g., source and destination IP address and port number)

PS based services: In WLAN interworking, PS based service is a general term to refer to the services provided by a PLMN using IP bearer capability between WLAN UEs and the PLMN in scenario 3 and upwards. They include all services provided by 3G PS domain that use the IP bearer service, (e.g., IMS, Internet access, Corporate IP network access), and other services (e.g., SMS and LCS).

********** MODIFIED SECTION **********

6.2.5 WLAN Access Gateway

The WLAN Access Gateway applies to scenario-3.

The WLAN Access Gateway is a gateway via which the data to/from the WLAN Access Network shall be routed via a PLMN to provide a WLAN UE with 3G PS based services in scenario 3.

The WLAN Access Gateway shall reside in the VPLMN in the roaming case, and in the HPLMN in the non-roaming case.

The WLAN Access Gateway:

- Allows VPLMN to generate charging information for users accessing via the WLAN AN in the roaming case.
- Enforces routing of packets through the PDG.
- Performs collection of per tunnel accounting information, e.g. volume count (byte count) and elapsed time, to be used for inter-operator settlements.
- Filters out packets based on unencrypted information in the packets. Packets should only be forwarded if they:

1. are part of an existing tunnel or
2. are expected messages from the WLAN UEs. This includes service requests, and tunnel establishment messages.

Since the WAG does not have a full trust relationship with the WLAN UE, it is not able to stop all messages. However, messages from an unknown IP address can easily be discarded. Other approaches may be used as well. Additional types of message screening are left to the operators' control. Furthermore, Network Address Translators within the WLAN may modify the source address of IP packets from the WLAN UEs. The modified source address can be reliably associated to a WLAN UE by the PDG during tunnel establishment and provided to the WAG via the 3GPP AAA Server/Proxy. Before this point, all tunnel establishment packets shall be routed by the WAG except those which are possibly discarded due to certain Firewall rules implemented on the WAG.

Note: per tunnel accounting generation in the WAG is not required when the WAG and PDG are in the same network, i.e. the non-roaming case.

The WAG may implement policy enforcement before tunnel establishment to enhance the firewall against unwanted packets go through the PLMN, for example, to forbid the roaming WLAN UE from sending tunnel establishment to PLMN other than its HPLMN; to forbid packets from unauthorized WLAN UE.

The WAG shall implement policy enforcement after tunnel establishment.

After tunnel establishment, the following procedures apply at the WAG:

- If service is provided through a PDG in the HPLMN the WAG:
  - Ensures that all packets from the WLAN UE are routed to the HPLMN.
  - Ensures that packets from the authorised WLAN UEs are only routed to the appropriate PDG in the HPLMN and that packets from other sources than that PDG are not routed to the WLAN UE.
- If service is provided through a PDG in the VPLMN the WAG:
  - Ensures that all packets from the WLAN UE are routed to the VPLMN.
  - Ensures that packets from the authorised WLAN UEs are only routed to the appropriate PDG in the VPLMN and that packets from other sources than that PDG are not routed to the WLAN UE.

6.2.5.1 ~~Routing~~ Policy Enforcement

Information regarding the selected PDG, including whether the PDG is in the HPLMN or the VPLMN is provided by the HPLMN to the VPLMN.

In the roaming case, the PDG information is delivered from the 3GPP AAA Server to the 3GPP AAA Proxy.

Within the VPLMN, policy enforcement information is delivered to the WAG.

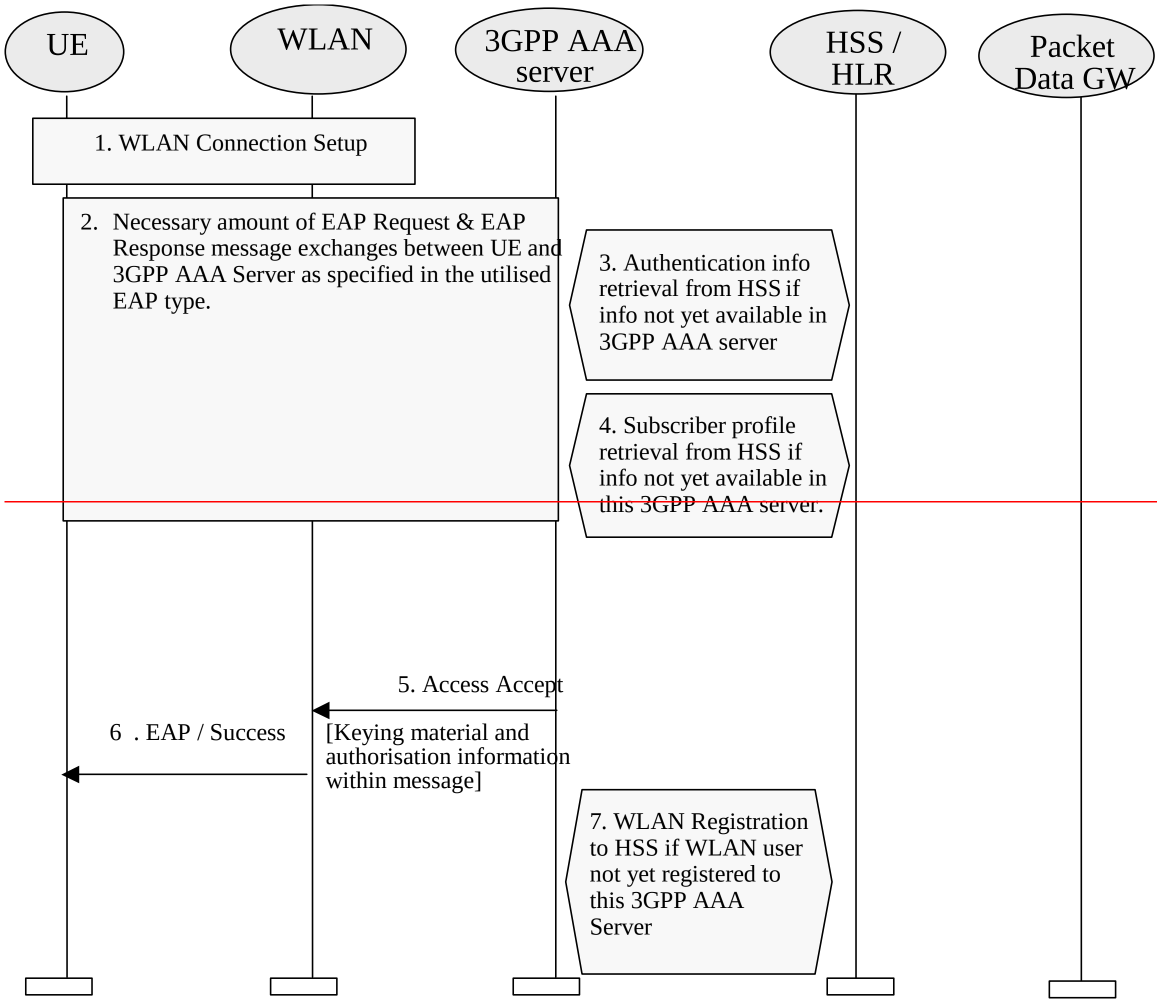
Note: Whether information regarding one or all PDGs is provided will likely impact the signalling which supports the activation of a further W-APN. Delivering information of all valid PDGs may limit impacts on signalling for further W-APN establishment.

The policy enforcement delivered during initial authentication (before the tunnel establishment) will be bound to a user's AAA signalling. The WAG requires functionality to be able to associate ~~securely bind~~ this information to a user's traffic. As an implementation option, this functionality can be achieved by allocating the local IP Address by VPLMN.

The binding of the policy to a user's traffic allows the WAG to drop un-authorized packets sent to/from a user.

********** MODIFIED SECTION **********

7.2 WLAN Access Authentication and Authorisation


UE
WLAN
3GPP AAA server
HSS / HLR
Packet Data GW
1. WLAN Connection Setup
2. Necessary amount of EAP Request & EAP Response message exchanges between UE and 3GPP AAA Server as specified in the utilised EAP type.
3. Authentication info retrieval from HSS if info not yet available in 3GPP AAA server
4. Subscriber profile retrieval from HSS if info not yet available in this 3GPP AAA server.
5. Access Accept
[Keying material and authorisation information within message]
6 . EAP / Success
7. WLAN Registration to HSS if WLAN user not yet registered to this 3GPP AAA Server

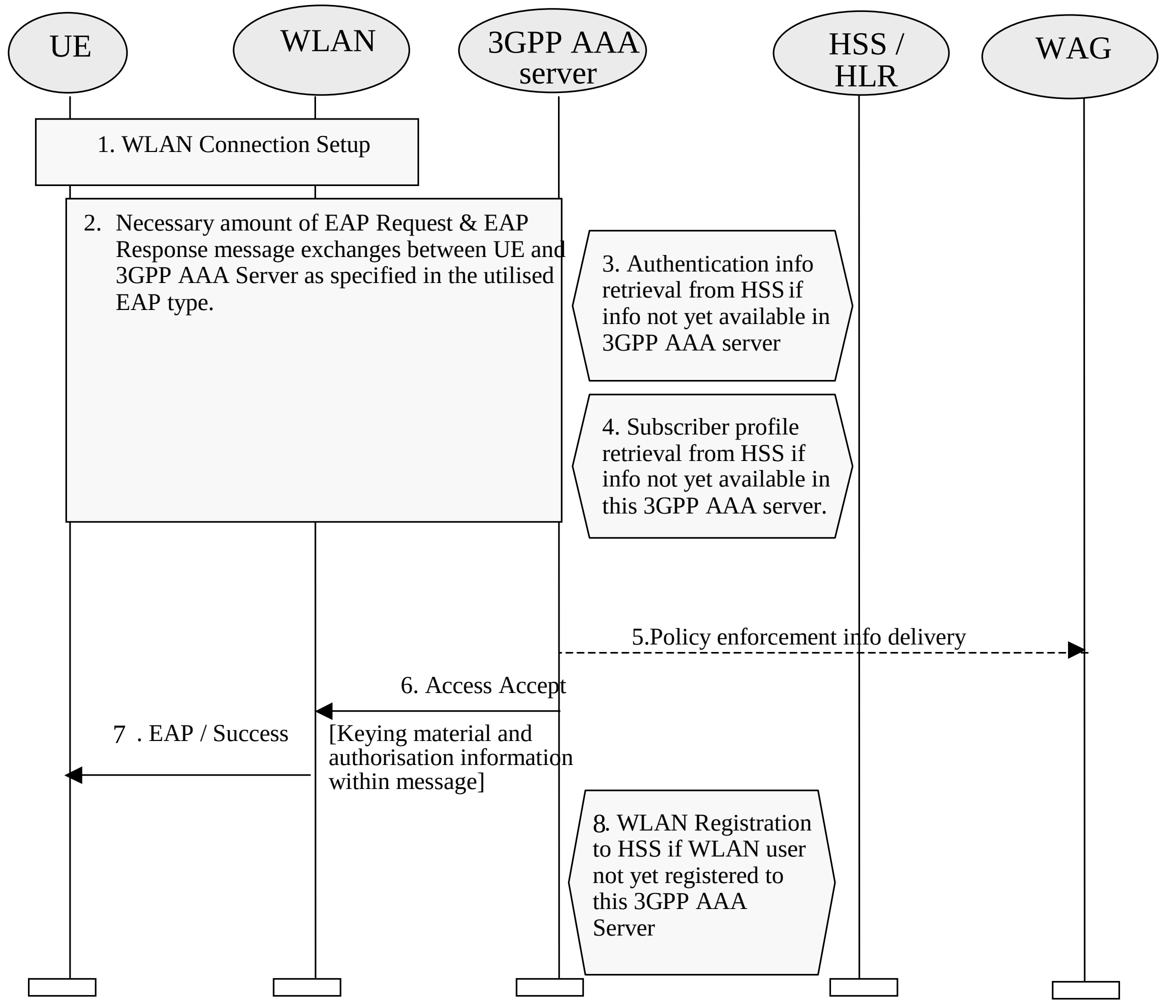

UE
WLAN
3GPP AAA server
HSS / HLR
WAG
1. WLAN Connection Setup
2. Necessary amount of EAP Request & EAP Response message exchanges between UE and 3GPP AAA Server as specified in the utilised EAP type.
3. Authentication info retrieval from HSS if info not yet available in 3GPP AAA server
4. Subscriber profile retrieval from HSS if info not yet available in this 3GPP AAA server.
5.Policy enforcement info delivery
6. Access Accept
7 . EAP / Success
[Keying material and authorisation information within message]
8. WLAN Registration to HSS if WLAN user not yet registered to this 3GPP AAA Server

Figure 7.1 Authentication and authorisation procedure

1. WLAN connection is established with a WLAN technology specific procedure (out of scope for 3GPP).
2. The EAP authentication procedure is initiated in WLAN technology specific way.

   All EAP packets are transported over the WLAN interface encapsulated within a WLAN technology specific protocol.

   All EAP packets are transported over the Wa reference point.

A number of EAP Request and EAP Response message exchanges is executed between 3GPP AAA Server and WLAN UE. The amount of round trips depends e.g. on the utilised EAP type. Information stored in and retrieved from HSS may be needed to execute certain EAP message exchanges.

3 Information to execute the authentication with the accessed user is retrieved from HSS. This information retrieval is needed only if necessary information to execute the EAP authentication is not already available in 3GPP AAA Server. To identify the user the *username* part of the provided NAI identity is utilised.

4 Subscribers WLAN related profile is retrieved from HSS. This profile includes e.g. the authorisation information and permanent identity of the user. Retrieval is needed only if subscriber profile information is not already available in 3GPP AAA Server.

5. Optionally, the 3GPP AAA server (or the 3GPP AAA proxy in roaming case) may send the policy enforcement information to the WAG in the PLMN that the WLAN UE selected in case VPLMN is to allocate the local IP Address for the WLAN UE.

Note: Additional process, such as allocating the IP address, may be necessary during or before this step to be performed.

~~5~~6. If the EAP authentication and authorisation was successful, then 3GPP AAA Server sends Access Accept message to WLAN. In this message 3GPP AAA Server includes EAP Success message, keying material derived from the EAP authentication as well as connection authorisation information (e.g. NAS Filter Rule or Tunnelling attributes) to the WLAN.

WLAN stores the keying material and authorisation information to be used in communication with the authenticated WLAN UE.

~~6~~7. WLAN informs the WLAN UE about the successful authentication and authorisation with the EAP Success message.

~~7~~8. 3GPP AAA server registers the WLAN users 3GPP AAA Server to the HSS. In registration messages the subscriber is identified by his permanent identity. This registration is needed only if the subscriber is not already registered to this 3GPP AAA Server.

3GPP TSG-SA WG2 Meeting #40
Sophia-Antipolis, France, 17-21 May 2004

Tdoc ⌘S2-041811

CR-Form-v7

CHANGE REQUEST

⌘	**23.234**	**CR**	**036**	⌘ **rev**	**-**	⌘	Current version:	**6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Reference to 23.825		
Source:	⌘	SA2 (Siemens)		
Work item code:	⌘	WLAN	***Date:*** ⌘	12/05/2004
Category:	⌘	**F**	***Release:*** ⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Current TS 23.234 contains a reference to TR 23.825 on IP flow based bearer level charging. However, this TR is frozen and the IP flow based charging work is continued in TS 23.125.
Summary of change:	⌘	Change reference to 23.825 into reference to 23.125 and add a reference to this specification to chapter 6.2.6.
Consequences if not approved:	⌘	Wrong reference in chapter 2 of TS 23.234.

Clauses affected:	⌘	2, 6.2.6			
		Y	**N**		
Other specs affected:	⌘		**X**	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

********** FIRST MODIFIED SECTION **********

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.101: "Service principles".

[3] 3GPP TR 22.934: "Feasibility study on 3GPP system to WLAN interworking".

[4] 3GPP TS 23.002: "Network architecture".

[5] 3GPP TS 23.003: "Numbering, addressing and identification".

[6] 3GPP TS 23.040: "Technical Realisation of the Short Message Service (SMS)"

[7] 3GPP TS 23.060: "GPRS; Service description".

[8] 3GPP TR 23.934: "3GPP system to WLAN Interworking; Functional and architectural definition".

[9] 3GPP TS 24.234: "3GPP System to WLAN Interworking; UE to Network protocols; Stage 3".

[10] 3GPP TS 29.002: "Mobile Application Part (MAP) specification".

[11] 3GPP TS 29.329: " Sh Interface based on the Diameter protocol; Protocol details".

[12] 3GPP TS 31.102: "Characteristics of the USIM Application."

[13] 3GPP TS 32.225: "Telecommunication management; Charging management; Charging data description for the IP Multimedia Subsystem (IMS)."

[14] 3GPP TS 33.234: "WLAN Interworking Security."

[15] 3GPP TS~~R~~ 23.~~8~~125: "Overall High Level Functionality and Architecture ~~Aspects~~Impacts of ~~IP~~ Flow Based ~~Bearer Level~~ Charging"

[16] RFC2284: "PPP Extensible Authentication Protocol (EAP)"

[17] RFC 2486: "The Network Access Identifier"

[18] J. Caron, "DNS Based Roaming", http://www.ietf.org/internet-drafts/draft-caron-dns-based-roaming-00.txt, April 2002, (work in progress)

[19] IEEE Std 802.1X-2001 IEEE Standard for Local and metropolitan area networks— Port-Based Network Access Control

[20] IETF Internet-Draft: "Network Discovery and Selection within the EAP Framework". draft-adrangi-eap-network-discovery-and-selection-01, work in progress.

[21] IEEE Std 802.11-1999, Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, IEEE, Sep. 1999.

[22] IETF Internet-Draft: "EAP AKA Authentication" draft-arkko-pppext-eap-aka-11 (October 2003).

[23] IETF Internet-Draft: "EAP SIM Authentication" draft-haverinen-pppext-eap-sim-12 (October 2003).

********** NEXT MODIFIED SECTION **********

6.2.6 Packet Data Gateway

The Packet Data Gateway applies to scenario-3.

3GPP PS based services (Scenario 3) are accessed via a Packet Data Gateway. 3GPP PS based services may be accessed via a Packet Data Gateway in the user's Home Network or a PDG in the selected VPLMN. The process of authorisation and service selection (e.g. W-APN selection) and subscription checking determines whether a service shall be provided by the home network or by the visited network. The resolution of the IP address of the Packet Data Gateway providing access to the selected service will be performed in the PLMN functioning as the home network (in the VPLMN or HPLMN).

Successful activation of a selected service results in:

- Determination of the Packet Data Gateway IP address used by the WLAN UE;
- Allocation of a WLAN UE's remote IP address to the WLAN UE (if one is not already allocated);
- Registration of the WLAN UE's local IP address with the Packet Data Gateway and binding of this address with the WLAN UE's remote IP address.

The Packet Data Gateway:

- Contains routeing information for WLAN-3G connected users;
- Routes the packet data received from/sent to the PDN to/from the WLAN-3G connected user;
- Performs address translation and mapping;
- Performs de-capsulation and encapsulation;
- accepts or rejects the requested W-APN according to the decision made by the 3GPP AAA Server;
- redirects the tunnel establishment request towards another PDG if this is indicated to be done by the 3GPP AAA Server

Allows allocation of the WLAN UE's remote IP address;

- Relays the WLAN UE's remote IP address allocated by an external IP network to the WLAN UE, when external IP network address allocation is used.
- Performs registration of the WLAN UE's local IP address and binding of this address with the WLAN UE's remote IP address;
- Provides procedures for unbinding a WLAN UE's local IP address with the WLAN UE's remote IP address;
- Provides procedures for authentication and prevention of hijacking (i.e. ensuring the validity of the WLAN UE initiating any binding of the WLAN UE's local IP address with the WLAN UE's remote IP address, unbinding etc.)
- May filter out unauthorised or unsolicited traffic with packet filtering functions. All types of message screening are left to the operators' control, e.g. by use of Internet firewalls.

- Generates per user charging information.

- Generates charging information related to user data traffic for offline and online charging purposes.

- May apply IP flow based bearer level charging [13], [15], e.g. in order to differentiate or suppress WLAN bearer charging for 3GPP PS based services.

- Performs the functions of Service-based Local Policy Enforcement Point (controls the quality of service that is provided to a set of IP flow as defined by a packet classifier, control admission based on policy that is applied to the IP bearers associated with the flow, and configuration of the packet handling and "gating" functionality in the user plane.)

- Communicates with Policy Decision Function (PDF) to allow service-based local policy and QoS inter-working information to be "pushed" by the PDF or to be requested by the PDG. This communication also provides information to support the following functions in the PDG:

  - Control of Diffserv inter-working;

  - Control of RSVP admission control and inter-working;

  - Control of "gating" function in PDG;

  - WLAN bearer authorization;

  - QoS charging related function.

3GPP TSG-SA WG2 Meeting #40
Sophia-Antipolis, France, 17-21 May 2004

Tdoc ⌘S2-042219

CR-Form-v7

CHANGE REQUEST

⌘	**23.234**	**CR**	**038**	⌘ **rev**	**2**	⌘	Current version:	**6.0.0**	⌘

For ***HELP*** *on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network ☒

Title:	⌘	Considerations on the format of the IP address used for tunnel establishment		
Source:	⌘	SA2 (Siemens)		
Work item code:	⌘	WLAN	***Date:*** ⌘	19/05/2004
Category:	⌘	**F**	***Release:*** ⌘	Rel-6
		Use one of the following categories: ***F*** *(correction)* ***A*** *(corresponds to a correction in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)* Detailed explanations of the above categories can be found in 3GPP TR 21.900.		*Use one of the following releases:* *2 (GSM Phase 2)* *R96 (Release 1996)* *R97 (Release 1997)* *R98 (Release 1998)* *R99 (Release 1999)* *Rel-4 (Release 4)* *Rel-5 (Release 5)* *Rel-6 (Release 6)*

Reason for change:	⌘	Chapter 5.7.2 of TS 23.234 requires that “The tunnel protocol shall be able to support IPv4 and IPv6 transport addresses”. This is due to the fact that in principle the WLAN AN can support Ipv4 and Ipv6 addresses. Thus, depending on the IP address version used in WLAN AN the WLAN UE has to establish a tunnel to the PDG with an Ipv4 or Ipv6 local address. On the other hand, the UE determines the tunnel endpoint address by DNS taking a certain W-APN and resolving it to an IP address. Clearly, the IP addresses at the two tunnel endpoints must be either of type Ipv4 or Ipv6. As the W-APN is usually a statically configured FQDN and the network does not know in advance the type of local address the WLAN UE is using, the DNS system should return an Ipv4 and Ipv6 address to the WLAN UE. The WLAN UE should choose the corresponding address and establish the tunnel to the PDG. As it would not be reasonable to implement and deploy PDGs exclusively for Ipv4 access and others for Ipv6 access a PDG should be supplied with a dual Ipv4/Ipv6 stack.
Summary of change:	⌘	Define the behaviour of the WLAN UE before tunnel establishment with respect to the format of the local IP address. Recommend that PDG and WLAN UE are equipped with a dual IP stack and that DNS should return an Ipv4 and Ipv6 address for a W-APN.
Consequences if not approved:	⌘	Inclompete description of 3GPP PS Access scenario and therefore missing guidance for stage 3.

Clauses affected:	⌘	6.2.1, 6.2.6, 7.9, 7.9.3
		Y **N**

Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

********** FIRST MODIFIED SECTION **********

6.2.1 WLAN UE

A WLAN UE is the UE (equipped with UICC card including (U)SIM) utilized by a 3GPP subscriber to access the WLAN network for 3GPP interworking purpose. A WLAN UE may include terminal types whose configuration (e.g. interface to a UICC), operation and software environment are not under the exclusive control of the 3GPP system operator, such as a laptop computer or PDA with a WLAN card, UICC card reader and suitable software applications.

The WLAN UE functions include:

- Associating to an I-WLAN.
- WLAN access authentication based on EAP methods.
- Selection of a suitable VPLMN in the roaming case.
- Building an appropriate NAI.
- Obtain a local IP address. If the WLAN UE is intended for use with WLAN ANs supporting IPv4 only as well as with WLAN ANs supporting IPv6 only, it shall be equipped with a dual IP stack.
- Building an appropriate W-APN to be used in scenario 3.
- Request the resolution of a W-APN in scenario 3 to a PDG address.
- If IPv4 and IPv6 addresses are returned during the resolution process, the WLAN UE shall select the address that has the same format as its own local IP address (IPv4 or IPv6).
- Establish a secure tunnel in scenario 3 to a PDG.
- Obtain a remote IP address to be used in scenario 3.
- Accessing services provided in the operators PS domain.
- Allowing users to select the type of network access, i.e.between direct access to external IP networks from the WLAN AN and network access through PLMN.

********** NEXT MODIFIED SECTION **********

6.2.6 Packet Data Gateway

The Packet Data Gateway applies to scenario-3.

3GPP PS based services (Scenario 3) are accessed via a Packet Data Gateway. 3GPP PS based services may be accessed via a Packet Data Gateway in the user's Home Network or a PDG in the selected VPLMN. The process of authorisation and service selection (e.g. W-APN selection) and subscription checking determines whether a service shall be provided by the home network or by the visited network. The resolution of the IP address of the Packet Data Gateway providing access to the selected service will be performed in the PLMN functioning as the home network (in the VPLMN or HPLMN). If the PDG is intended to support connections from WLAN UEs using IPv4 and IPv6 local addresses, it shall be equipped with a dual IP stack.

Successful activation of a selected service results in:

- Determination of the Packet Data Gateway IP address used by the WLAN UE;

- Allocation of a WLAN UE's remote IP address to the WLAN UE (if one is not already allocated);
- Registration of the WLAN UE's local IP address with the Packet Data Gateway and binding of this address with the WLAN UE's remote IP address.

The Packet Data Gateway:

- Contains routeing information for WLAN-3G connected users;
- Routes the packet data received from/sent to the PDN to/from the WLAN-3G connected user;
- Performs address translation and mapping;
- Performs de-capsulation and encapsulation;
- accepts or rejects the requested W-APN according to the decision made by the 3GPP AAA Server;
- redirects the tunnel establishment request towards another PDG if this is indicated to be done by the 3GPP AAA Server

Allows allocation of the WLAN UE's remote IP address;

- Relays the WLAN UE's remote IP address allocated by an external IP network to the WLAN UE, when external IP network address allocation is used.
- Performs registration of the WLAN UE's local IP address and binding of this address with the WLAN UE's remote IP address;
- Provides procedures for unbinding a WLAN UE's local IP address with the WLAN UE's remote IP address;
- Provides procedures for authentication and prevention of hijacking (i.e. ensuring the validity of the WLAN UE initiating any binding of the WLAN UE's local IP address with the WLAN UE's remote IP address, unbinding etc.)
- May filter out unauthorised or unsolicited traffic with packet filtering functions. All types of message screening are left to the operators' control, e.g. by use of Internet firewalls.
- Generates per user charging information.
- Generates charging information related to user data traffic for offline and online charging purposes.
- May apply IP flow based bearer level charging [13], e.g. in order to differentiate or suppress WLAN bearer charging for 3GPP PS based services.
- Performs the functions of Service-based Local Policy Enforcement Point (controls the quality of service that is provided to a set of IP flow as defined by a packet classifier, control admission based on policy that is applied to the IP bearers associated with the flow, and configuration of the packet handling and "gating" functionality in the user plane.)
- Communicates with Policy Decision Function (PDF) to allow service-based local policy and QoS inter-working information to be "pushed" by the PDF or to be requested by the PDG. This communication also provides information to support the following functions in the PDG:
    - Control of Diffserv inter-working;
    - Control of RSVP admission control and inter-working;
    - Control of "gating" function in PDG;
    - WLAN bearer authorization;
    - QoS charging related function.

********** NEXT MODIFIED SECTION **********

7.9 W-APN resolution and Tunnel establishment

This information flow presents the generic message exchange necessary in order to resolve the selected W-APN and establish a WLAN UE-Initiated tunnel for Scenario 3 purposes.

As a prerequisite of these procedures it is necessary to perform the following:

1. WLAN Access Authentication and Authorisation and provisioning of the WLAN UE's local IP address

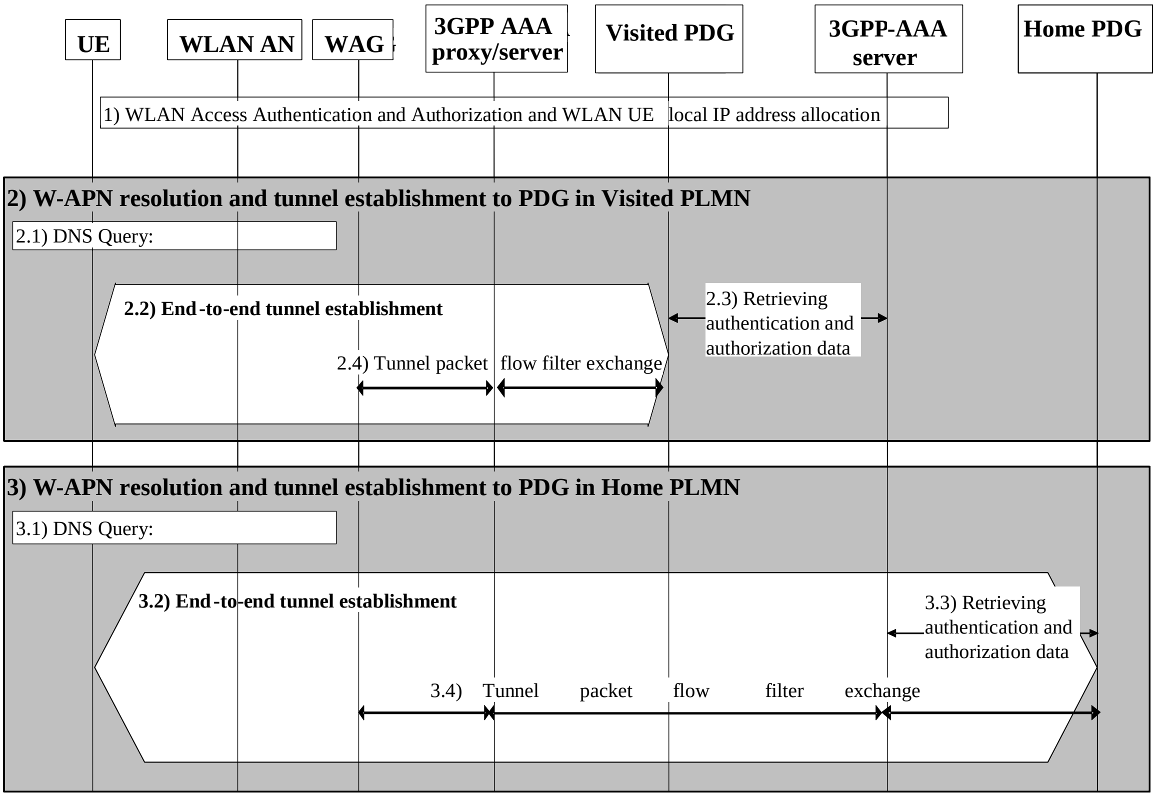

UE
WLAN AN
WAG
3GPP AAA proxy/server
Visited PDG
3GPP-AAA server
Home PDG
1) WLAN Access Authentication and Authorization and WLAN UE local IP address allocation
2) W-APN resolution and tunnel establishment to PDG in Visited PLMN
2.1) DNS Query:
2.2) End-to-end tunnel establishment
2.3) Retrieving authentication and authorization data
2.4) Tunnel packet flow filter exchange
3) W-APN resolution and tunnel establishment to PDG in Home PLMN
3.1) DNS Query:
3.2) End-to-end tunnel establishment
3.3) Retrieving authentication and authorization data
3.4) Tunnel packet flow filter exchange

Figure 7.10: Example message flow to WLAN UE-Initiated tunnel establishment

When the user decides that he wants to access a service, the WLAN UE selects the W-APN network ID associated to the service requested by the user.

A detailed description of the W-APN resolution and the WLAN UE-Initiated Tunnel Establishment is given below.

2. Depending on internal configuration, the WLAN UE initiates W-APN resolution and tunnel establishment with a PDG in VPLMN.

Note: The configuration of the WLAN UE regarding W-APNs can be controlled by e.g. USIM Application Toolkit-based mechanisms.

2.1 WLAN UE constructs an FQDN using the W-APN Network Identifier and VPLMN ID as the Operator Identifier and performs a DNS query to resolve it. The DNS response will contain one or more IP addresses of equivalent PDGs that support the requested W-APN in the VPLMN according to standard DNS procedures.
If the VPLMN does not support the W-APN, then the DNS query returns a negative response. In this case, the WLAN UE continues with step 3.

2.2 The WLAN UE selects a PDG from the list received in step 2.1. If the DNS response contains IPv4 and IPv6 adresses, the WLAN UE has to select an address that has the same format as its own local IP address.~~, and~~ If a PDG is finally selected, the establishment of an end-to-end tunnel is performed between the WLAN UE and this PDG~~s~~. The WLAN UE shall include the W-APN and the user identity in the initial tunnel establishment request.

2.3 During the tunnel establishment, the PDG contacts the 3GPP AAA Server in the HPLMN via the 3GPP AAA proxy for authorization of the WLAN UE and to retrieve the information required for the mutual authentication part of the tunnel establishment.
The 3GPP AAA Server verifies that the user requesting the tunnel establishment has been already successfully WLAN Access Authorized. If not, the tunnel establishment request is rejected.
If the WLAN UE is not allowed to use a visited-PDG to access the given W-APN, then the tunnel establishment shall be rejected by the PDG.

If it is not possible to establish the tunnel with any of the PDGs recieved from step 2.1, or the tunnel establishment failure reason is that the WLAN UE is not allowed to use a visited-PDG to access the given W-APN, then the WLAN UE continues with step 3.

2.4 During the tunnel establishment procedure, the PDG and the WAG exchange information via the 3GPP AAA Proxy in order to establish a filtering policy to allow the forwarding of tunnelled packets to the PDG. The 3GPP AAA Proxy requests the WAG to apply filtering policy based on information obtained from the PDG. The 3GPP AAA Proxy decides which filtering policy could be applied by the WAG according to local information (e.g. based on number of users, WAG capabilities, roaming agreement policy, etc).

3. Depending on internal configuration, or due to the failure of step 2.1 or 2.3, the WLAN UE initiates W-APN resolution and tunnel establishment with a PDG in HPLMN.

3.1 WLAN UE constructs an FQDN using W-APN Network Identifier and the HPLMN ID as the Operator Identifier, and performs a DNS query to resolve it. The DNS response will contain one or more IP addresses of equivalent PDGs that support the requested W-APN in the HPLMN according to standard DNS procedures.

3.2 The WLAN UE selects a PDG from the list received in step 3.1. If the DNS response contains IPv4 and IPv6 addresses, the WLAN UE has to select an address that has the same format as its own local IP address.~~, and the~~ If a PDG is finally selected, establishment of an end-to-end tunnel is performed between the WLAN UE and this PDG~~s~~. The WLAN UE shall include the W-APN and the user identity in the initial tunnel establishment request.

3.3 During the tunnel establishment, the PDG contacts the 3GPP AAA Server in the HPLMN for authorization of the WLAN UE and to retrieve the information required for the mutual authentication part of tunnel establishment. The 3GPP AAA Server verifies that the user requesting the tunnel establishment has been already WLAN Access Authorized. If not, the tunnel establishment request is rejected.
If the WLAN UE is not allowed to use a Home PDG to access the given W-APN according to his subscription, then the tunnel establishment shall be rejected by the Home PDG.

3.4 During the tunnel establishment, the PDG and the WAG exchange information via the 3GPP AAA Server and 3GPP AAA Proxy in order to establish a filtering policy to allow the forwarding of tunnelled packets to the PDG. The 3GPP AAA server requests to the WAG to apply filtering policy based on information obtained from the PDG. The 3GPP AAA server decides which filtering policy could be applied by the WAG according to local information (e.g. based on number of user, WAG capabilities, roaming agreement policy, etc). The applied filtering policy is communicated to the Home-PDG.

********** NEXT MODIFIED SECTION **********

7.9.3 Use of DNS

It shall be possible to restrict the propagation of DNS information used for the above mechanism to DNS servers controlled by the PLMNs and to DNS servers available only to authorised 3GPP WLAN UEs (i.e. those WLAN UEs which have successfully connected to a 3GPP Interworking WLAN.)

It shall be possible to configure multiple PDG addresses against a single FQDN in a manner which allows the load to be shared across these PDGs.

It shall be possible to configure IPv4 and IPv6 addresses against a single FQDN and to return these addresses together to the WLAN UE.

Note: The above shall be achieved by standard DNS mechanisms. The usage of TLD and the DNS query performed by the WLAN UE to resolve the W-APN are left to stage 3. Further details are in [5]**.**

3GPP TSG-SA2 Meeting #40
Sofia Antipolis, France, 17th – 21st May 2004

Tdoc ⌘ S2-042225

CR-Form-v7

CHANGE REQUEST

⌘	**23.234**	**CR**	**041**	⌘ **rev**	**2**	⌘	Current version:	**6.0.0** ⌘

For ***HELP*** *on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME □ Radio Access Network □ Core Network ☒

Title:	⌘	Per-user charging in the VPLMN		
Source:	⌘	SA2 (T-Mobile, Samsung)		
Work item code:	⌘	WLAN	***Date:*** ⌘	11/05/2004
Category:	⌘	**F**	***Release:*** ⌘	Rel-6

Use one of the following categories:
- ***F*** *(correction)*
- ***A*** *(corresponds to a correction in an earlier release)*
- ***B*** *(addition of feature),*
- ***C*** *(functional modification of feature)*
- ***D*** *(editorial modification)*

Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Per-User charging in the VPLMN is mentioned as necessary functionality and requirement, but the mechanism of how the User Identifier is transported to the VPLMN is missing
Summary of change:	⌘	Add the information on how the User Identifier is transported to the VPLMN (AAA Proxy)
Consequences if not approved:	⌘	The VPLMN will not be able to provide a User Identifier in the per-user charging records

Clauses affected:	⌘	3.1, 6.2.2, 6.2.6, 6.3.6, 6.3.10, 6.3.11.2

		Y	**N**		
Other specs affected:	⌘		**X**	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

First modified section

3.1 Definitions

Available SSID: It is an SSID that the WLAN UE has found after active and/or passive scanning which meets certain conditions as specified in IEEE 802.11 [19].

3GPP - WLAN Interworking: Used generically to refer to interworking between the 3GPP system and the WLAN family of standards**.** Annex B includes examples of WLAN Radio Network Technologies.

Environment: The type of area to be covered by the WLAN network of a 3GPP - WLAN interworking; e.g. public, corporate and residential.

External IP Network/External Packet Data Network: An IP network to which access may be provided through the 3GPP system, rather than directly from the WLAN AN. For example, the Internet, an operator's IP network or a 3rd party IP network such as a corporate IP network.

Home WLAN: The WLAN that is interworking with the HPLMN of the 3GPP - WLAN interworking user.

Interworking WLAN : WLAN that interworks with a 3GPP system**.**

I-WLAN selection: Procedure for the selection among the available I-WLAN APs

Offline charging: Offline charging mechanism is provided for collecting and forwarding charging information about occurred WLAN access resource and core network resource usage, etc without affecting the service rendered in real-time.

Online charging: Online charging mechanism is provided where the service rendered is affected in real-time and is required for a direct interaction with session/service control. This allows an online charged subscriber to access WLAN.

Policy Enforcement: In scenario 3, Policy Enforcement is implemented in a WAG to allow only authorized packets to/from a WLAN AN to pass through.

PS based services: In WLAN interworking, PS based service is a general term to refer to the services provided by a PLMN using IP bearer capability between WLAN UEs and the PLMN in scenario 3 and upwards. They include all services provided by 3G PS domain that use the IP bearer service, (e.g., IMS, Internet access, Corporate IP network access), and other services (e.g., SMS and LCS).

Requested W-APN: The W-APN requested by the user

Routing Enforcement: In scenario 3, Routing Enforcement ensures that all packets sent to/from the WLAN UE for 3G PS based service are routed to the interworking VPLMN (roaming case) or HPLMN (no roaming case). Routing Enforcement is implemented between a WLAN AN and a WAG.

Selected W-APN: The W-APN selected by the network as a result of the user request

Service Authorization: Authorization for a user to access the requested service according to the user's subscription.

Supported PLMN: A PLMN of a roaming partner (i.e. to which the WLAN operator has a direct roaming relationship).

Tunnel Identifier: Identifier of an end to end tunnel between a UE and a PDG. It is contained in the unencrypted part of the packets

User Identifier: Identifier of a user used for e.g. charging functionality

Visited WLAN: An interworking WLAN that Interworks only with a visited PLMN.

W-APN: WLAN Access Point Name – identifies an IP network and a point of interconnection to that network (Packet Data Gateway)

WLAN coverage: an area where wireless local area network access services are provided for interworking by an entity in accordance with WLAN standards.

WLAN roaming: The ability for a 3GPP - WLAN interworking user (subscriber) to function in a serving WLAN different from the home WLAN

WLAN UE: The WLAN UE is the UE (equipped with UICC card including (U)SIM) utilized by a 3GPP subscriber to access the WLAN interworking.

WLAN UE's local IP address: An address that is necessary to deliver the packet to a WLAN UE in a WLAN AN. It identifies the WLAN UE in the WLAN AN. WLAN UE's local IP address may be translated by Network Address Translation prior to being received by the interworking function.

WLAN UE's remote IP address: An address used in the data packet encapsulated by the WLAN UE-initiated tunnel. It represents the identity of the WLAN UE in the network which the WLAN UE is accessing.

Second modified section

6.2.2 3GPP AAA Proxy

The 3GPP AAA Proxy represents a proxying and filtering function that resides in the Visited 3GPP Network. The 3GPP AAA Proxy functions include:

- Relaying the AAA information between WLAN and the 3GPP AAA Server.
- Enforcing policies derived from roaming agreements between 3GPP operators and between WLAN operator and 3GPP operator
- Reporting per-user charging/accounting information to the VPLMN CCF/CGw for roaming users
- Service termination (O&M initiated termination from visited network operator)
- Protocol conversion when the Wa and Wd reference points do not use the same protocol

For Scenario 3 only:

- Receiving per-tunnel charging information based on the tunnel identifier from the WAG and mapping of a user identifier and a tunnel identifier from the PDG; generating per user charging records for roaming users.
- Receiving authorization information related to subscriber requests for W-APNs in the Home or Visited network
- Authorization of access to Visited network W-APNs according to local policy

The 3GPP AAA Proxy functionality can reside in a separate physical network node, it may reside in the 3GPP AAA Server or any other physical network node.

Third modified section

6.2.6 Packet Data Gateway

The Packet Data Gateway applies to scenario-3.

3GPP PS based services (Scenario 3) are accessed via a Packet Data Gateway. 3GPP PS based services may be accessed via a Packet Data Gateway in the user's Home Network or a PDG in the selected VPLMN. The process of authorisation and service selection (e.g. W-APN selection) and subscription checking determines whether a service shall be provided by the home network or by the visited network. The resolution of the IP address of the Packet Data Gateway providing access to the selected service will be performed in the PLMN functioning as the home network (in the VPLMN or HPLMN).

Successful activation of a selected service results in:

- Determination of the Packet Data Gateway IP address used by the WLAN UE;
- Allocation of a WLAN UE's remote IP address to the WLAN UE (if one is not already allocated);
- Registration of the WLAN UE's local IP address with the Packet Data Gateway and binding of this address with the WLAN UE's remote IP address.

The Packet Data Gateway:

- Contains routeing information for WLAN-3G connected users;
- Routes the packet data received from/sent to the PDN to/from the WLAN-3G connected user;
- Performs address translation and mapping;
- Performs de-capsulation and encapsulation;
- accepts or rejects the requested W-APN according to the decision made by the 3GPP AAA Server;
- redirects the tunnel establishment request towards another PDG if this is indicated to be done by the 3GPP AAA Server

Allows allocation of the WLAN UE's remote IP address;

- Relays the WLAN UE's remote IP address allocated by an external IP network to the WLAN UE, when external IP network address allocation is used.
- Performs registration of the WLAN UE's local IP address and binding of this address with the WLAN UE's remote IP address;
- Provides procedures for unbinding a WLAN UE's local IP address with the WLAN UE's remote IP address;
- Provides procedures for authentication and prevention of hijacking (i.e. ensuring the validity of the WLAN UE initiating any binding of the WLAN UE's local IP address with the WLAN UE's remote IP address, unbinding etc.)
- May filter out unauthorised or unsolicited traffic with packet filtering functions. All types of message screening are left to the operators' control, e.g. by use of Internet firewalls.
- Generates per user charging information.
- Delivers the mapping of a user identifier and a tunnel identifier to the AAA Proxy.
- Generates charging information related to user data traffic for offline and online charging purposes.
- May apply IP flow based bearer level charging [13], e.g. in order to differentiate or suppress WLAN bearer charging for 3GPP PS based services.
- Performs the functions of Service-based Local Policy Enforcement Point (controls the quality of service that is provided to a set of IP flow as defined by a packet classifier, control admission based on policy that is applied to the IP bearers associated with the flow, and configuration of the packet handling and "gating" functionality in the user plane.)
- Communicates with Policy Decision Function (PDF) to allow service-based local policy and QoS inter-working information to be "pushed" by the PDF or to be requested by the PDG. This communication also provides information to support the following functions in the PDG:
    - Control of Diffserv inter-working;
    - Control of RSVP admission control and inter-working;
    - Control of "gating" function in PDG;
    - WLAN bearer authorization;
    - QoS charging related function;

Fourth modified section

6.3.6 Wg reference point

The Wg reference point applies to scenario-3.

This is an AAA interface between the 3GPP AAA Server/Proxy and the WAG. It is used to

- ~~p~~Provide information needed by the WAG to perform policy enforcement functions for authorised users.

- Transport per-tunnel based charging information from the WAG to the AAA Proxy.

Fifth modified section

6.3.10 Wm reference point

The Wm reference point applies to scenario-3.

This reference point is located between 3GPP AAA Server and Packet Data Gateway. The functionality of this reference point is to enable:

- The 3GPP AAA Server to retrieve tunneling attributes and WLAN UE's IP configuration parameters from/via Packet Data Gateway.
- Carrying messages for service authentication between WLAN UE and 3GPP AAA server.
- Carrying messages for service authorization between PDG and 3GPP AAA server.
- Carrying authentication data for the purpose of tunnel establishment, tunnel data authentication and encryption.
- Carrying mapping of a user identifier and a tunnel identifier sent from the PDG to the AAA Proxy through the AAA Server.

6.3.11 Wd reference point

6.3.11.1 General description

The Wd reference point connects the 3GPP AAA Proxy, possibly via intermediate networks, to the 3GPP AAA Server. The prime purpose of the protocols crossing this reference point is to transport authentication, authorization and related information in a secure manner.

EAP authentication shall be transported over the Wd reference point.

6.3.11.2 Functionality

The functionality of the reference point is to transport AAA messages including:

- Carrying data for authentication signalling between 3GPP AAA Proxy and 3GPP AAA Server
- Carrying data for authorization signalling between 3GPP AAA Proxy and 3GPP AAA Server
- Carrying charging signalling per WLAN user
- Carrying keying data for the purpose of radio interface integrity protection and encryption
- Carrying authentication data for the purpose of tunnel establishment, tunnel data authentication and encryption.
- Carrying mapping of a user identifier and a tunnel identifier sent from the PDG to the AAA Proxy through the AAA Server.
- Used for purging a user from the WLAN access for immediate service termination
- Enabling the identification of the operator networks amongst which the roaming occurs

3GPP TSG-SA WG2 Meeting #40
Sophia Antipolis, France, 17-21 May 2004

Tdoc ⌘S2-041862

CR-Form-v7

CHANGE REQUEST

⌘	**23.234**	**CR**	**043**	⌘**rev**	**2**	⌘	Current version:	**6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME □ Radio Access Network □ Core Network ☒

Title:	⌘	Roaming access to WLAN local services in Scenario 2		
Source:	⌘	SA2 (Nortel Networks)		
Work item code:	⌘	WLAN	***Date:*** ⌘	19/05/2004
Category:	⌘	**C**	***Release:*** ⌘	Rel-6
		Use one of the following categories: ***F*** *(correction)* ***A*** *(corresponds to a correction in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)* Detailed explanations of the above categories can be found in 3GPP TR 21.900.		*Use one of the following releases:* *2 (GSM Phase 2)* *R96 (Release 1996)* *R97 (Release 1997)* *R98 (Release 1998)* *R99 (Release 1999)* *Rel-4 (Release 4)* *Rel-5 (Release 5)* *Rel-6 (Release 6)*

Reason for change:	⌘	Internet Access is not the only service which may be accessed by a "Scenario 2" WLAN UE: TS 22.234 section 5.1.7.1 states: "3GPP based access control and charging. The user shall be able to access general internet services ***and/or corporate intranets***. (Scenario 2 of TR 22.934 [2])" TS 23.234 section 5.2 states: "WLAN Access rules/policy should be specified by the home and/or visited operator based on the subscriber's profile, the account status, O&M rules (e.g. blacklist, access limitation list), and local agreements. Factors such as access time and access location could also be considered in these rules. The access scope limitation could be, for example, only/not/may "access through WAG"; only/not/may "**access intranet X**". However, there are no means to specify the services (e.g. intranets) that the user is entitled to access in the Service Profile. Furthermore, whilst for the non-roaming case, the 3GPP AAA Server can interpret the Service Profile to derive appropriate access rules to be passed to the WLAN, the mechanism will not be sufficient for the roaming case, since the information about how to specify particular access rules to the WLAN (the actual filters to be applied) lies in the visited network.
Summary of change:	⌘	The Service Profile is updated to include a list of local services, e.g. corporate intranets, that the user is entitled to access directly from the WLAN.
Consequences if	⌘	

not approved:	

Clauses affected:	⌘	6.2.2, 6.3.1, 6.5, 7.2				
		Y	**N**			
Other specs affected:	⌘	**Y**		Other core specifications	⌘	Stage 3 specifications for Wd and Wx
			N	Test specifications		
			N	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

************************** Start of Changes ******************************

3.1 Definitions

Available SSID: It is an SSID that the WLAN UE has found after active and/or passive scanning which meets certain conditions as specified in IEEE 802.11 [19].

3GPP - WLAN Interworking: Used generically to refer to interworking between the 3GPP system and the WLAN family of standards**.** Annex B includes examples of WLAN Radio Network Technologies.

Environment: The type of area to be covered by the WLAN network of a 3GPP - WLAN interworking; e.g. public, corporate and residential.

External IP Network/External Packet Data Network: An IP network to which access may be provided through the 3GPP system, rather than directly from the WLAN AN. For example, the Internet, an operator's IP network or a 3rd party IP network such as a corporate IP network.

Home WLAN: The WLAN that is interworking with the HPLMN of the 3GPP - WLAN interworking user.

Interworking WLAN : WLAN that interworks with a 3GPP system**.**

I-WLAN selection: Procedure for the selection among the available I-WLAN Aps

Local Service Identifier: An identifier, used within the 3GPP system, for a service available directly from the I-WLAN, for example Internet access or access to a specific corporate network

Offline charging: Offline charging mechanism is provided for collecting and forwarding charging information about occurred WLAN access resource and core network resource usage, etc without affecting the service rendered in real-time.

Online charging: Online charging mechanism is provided where the service rendered is affected in real-time and is required for a direct interaction with session/service control. This allows an online charged subscriber to access WLAN.

Policy Enforcement: In scenario 3, Policy Enforcement is implemented in a WAG to allow only authorized packets to/from a WLAN AN to pass through.

PS based services: In WLAN interworking, PS based service is a general term to refer to the services provided by a PLMN using IP bearer capability between WLAN UEs and the PLMN in scenario 3 and upwards. They include all services provided by 3G PS domain that use the IP bearer service, (e.g., IMS, Internet access, Corporate IP network access), and other services (e.g., SMS and LCS).

Requested W-APN: The W-APN requested by the user

Routing Enforcement: In scenario 3, Routing Enforcement ensures that all packets sent to/from the WLAN UE for 3G PS based service are routed to the interworking VPLMN (roaming case) or HPLMN (no roaming case). Routing Enforcement is implemented between a WLAN AN and a WAG.

Selected W-APN: The W-APN selected by the network as a result of the user request

Service Authorization: Authorization for a user to access the requested service according to the user's subscription.

Supported PLMN: A PLMN of a roaming partner (i.e. to which the WLAN operator has a direct roaming relationship).

Visited WLAN: An interworking WLAN that Interworks only with a visited PLMN.

W-APN: WLAN Access Point Name – identifies an IP network and a point of interconnection to that network (Packet Data Gateway)

WLAN coverage: an area where wireless local area network access services are provided for interworking by an entity in accordance with WLAN standards.

WLAN roaming: The ability for a 3GPP - WLAN interworking user (subscriber) to function in a serving WLAN different from the home WLAN

WLAN UE: The WLAN UE is the UE (equipped with UICC card including (U)SIM) utilized by a 3GPP subscriber to access the WLAN interworking.

WLAN UE's local IP address:An address that is necessary to deliver the packet to a WLAN UE in a WLAN AN. It identifies the WLAN UE in the WLAN AN. WLAN UE's local IP address may be translated by Network Address Translation prior to being received by the interworking function.

WLAN UE's remote IP address: An address used in the data packet encapsulated by the WLAN UE-initiated tunnel. It represents the identity of the WLAN UE in the network which the WLAN UE is accessing.

*************************** Next Change *******************************

6.2.2 3GPP AAA Proxy

The 3GPP AAA Proxy represents a proxying and filtering function that resides in the Visited 3GPP Network. The 3GPP AAA Proxy functions include:

- Relaying the AAA information between WLAN and the 3GPP AAA Server.
- Enforcing policies derived from roaming agreements between 3GPP operators and between WLAN operator and 3GPP operator
- Providing access scope limitation information to the WLAN based on authorization information from the Home network
- Reporting per-user charging/accounting information to the VPLMN CCF/CGw for roaming users
- Service termination (O&M initiated termination from visited network operator)
- Protocol conversion when the Wa and Wd reference points do not use the same protocol

For Scenario 3 only:

- Receiving authorization information related to subscriber requests for W-APNs in the Home or Visited network
- Authorization of access to Visited network W-APNs according to local policy

The 3GPP AAA Proxy functionality can reside in a separate physical network node, it may reside in the 3GPP AAA Server or any other physical network node.

*************************** Next Change *******************************

6.3.1 Wa reference point

6.3.1.1 General description

The Wa reference point connects the WLAN Access Network, possibly via intermediate networks, to the 3GPP Network (i.e. the 3GPP AAA Proxy in the roaming case and the 3GPP AAA server in the non-roaming case). The prime purpose of the protocols crossing this reference point is to transport authentication, authorization and charging-related information in a secure manner. The reference point has to accommodate also legacy WLAN Access Networks.

Legacy logical nodes outside of 3GPP scope that terminate or proxy the Wa reference point signalling and do not support 3GPP AAA protocol shall require signalling conversion between the legacy AAA protocol and the 3GPP AAA protocol.

EAP authentication shall be transported over the Wa reference point.

6.3.1.2 Functionality

The functionality of the reference point is to transport AAA frames:

- Carrying data for authentication signalling between WLAN UE and 3GPP Network.
- Carrying data for authorization signalling between WLAN AN and 3GPP Network. These data may include a well-defined identification of the WLAN AN.
- Carrying charging signalling per WLAN user.
- Enabling the identification of the operator networks amongst which the roaming occurs.
- Carrying keying data for the purpose of radio interface integrity protection and encryption.
- When such functionality is supported by the WLAN AN, purging a user from the WLAN access for immediate service termination
- Providing access scope limitation information to the WLAN based on the authorised services for each user (for example, IP address filters)

To minimize the requirements put on the WLAN Access Network and to protect the confidentiality of the subscriber's charging status the fact whether a user is offline or online charged by his 3GPP subscription provider shall be transparent for the WLAN AN and thus for the Wa reference point.

************************** Next Change ******************************

6.5 WLAN user profile

The WLAN user profile shall reside in HSS (if the operator is using a legacy HLR, the WLAN user profile may reside in the 3GPP AAA Server) and be retrieved from AAA via Wx reference point. The profile shall contain the following data items: Detailed work on these parameters is expected in stage 3 work.

1. IMSI

   User identification.

2. MSISDN *(optional)*

   User identification, for example used for charging purposes

3. Operator determined barring of 3GPP-WLAN interworking subscription

4. Operator determined barring of 3GPP WLAN tunneling

   This allows operator to disable all W-APNs at one time. If there is a conflict between this item and the "access allowed" flag of any W-APN, the most restrictive will prevail.

5. Maximum session duration *(optional)*

   Used for re-authentication purposes. If this field is not used, the WLAN AN will apply default time intervals.

6. Charging mode (pre-paid, post-paid, both) and accounting server identifier(s) for every charging mode

   Charging mode to be applied and, for every case, the charging node where the accounting information is to be reported.

7. List of authorized W-APNs *(optional)*

   List of W-APNs for which the user will have services available. These W-APNs may correspond to services in the home network or in the visited network. Each W-APN shall have a flag indicating whether access is allowed in visited PLMNs or in the home PLMN.

8. Local access allowed

   Indicates ~~if the~~the local services that the user is allowed to have direct access to from the WLAN Access Network. ~~external IP networks~~, e.g. Internet,corporate Intranets ~~from the WLAN Access Network~~.
   ~~If this parameter should be further split down to specific services that are allowed or not from the WLAN AN is FFS~~ This is indicated in the form of a list of Local Service Identifiers~~.~~

NOTE: Local Service Identifiers are not passed outside the 3GPP system – access to services within the WLAN is restricted by means of access scope limitations applied on the Wa reference point.

NOTE: In the roaming case, Local Service Identifiers must be agreed between Home and Visited operators. A Local Service Identifier for Internet access should be specified at Stage 3. A Local Service Identifier for each corporate network should be specified at Stage 3.

9. Roaming allowed

   Indicates if the user is allowed to use 3GPP-WLAN Interworking in an WLAN AN that have no direct connection to the home PLMN.

************************** Next Change ******************************

7.2 WLAN Access Authentication and Authorisation

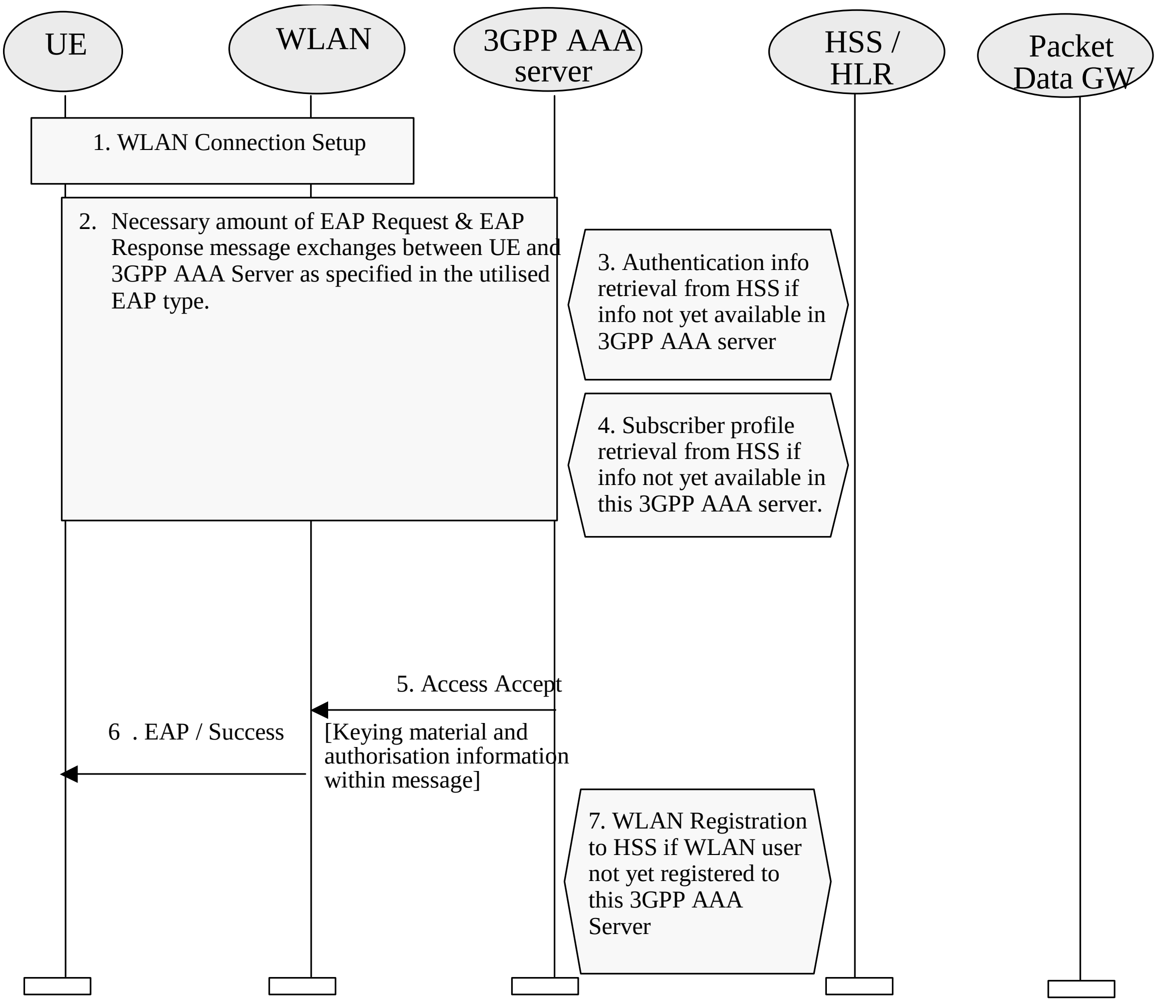

UE
WLAN
3GPP AAA server
HSS / HLR
Packet Data GW
1. WLAN Connection Setup
2. Necessary amount of EAP Request & EAP Response message exchanges between UE and 3GPP AAA Server as specified in the utilised EAP type.
3. Authentication info retrieval from HSS if info not yet available in 3GPP AAA server
4. Subscriber profile retrieval from HSS if info not yet available in this 3GPP AAA server.
5. Access Accept
[Keying material and authorisation information within message]
6 . EAP / Success
7. WLAN Registration to HSS if WLAN user not yet registered to this 3GPP AAA Server

Figure 7.2: Authentication and authorisation procedure

1. WLAN connection is established with a WLAN technology specific procedure (out of scope for 3GPP).

2. The EAP authentication procedure is initiated in WLAN technology specific way.

   All EAP packets are transported over the WLAN interface encapsulated within a WLAN technology specific protocol.

   All EAP packets are transported over the Wa reference point.

A number of EAP Request and EAP Response message exchanges is executed between 3GPP AAA Server and WLAN UE. The amount of round trips depends e.g. on the utilised EAP type. Information stored in and retrieved from HSS may be needed to execute certain EAP message exchanges.

3 Information to execute the authentication with the accessed user is retrieved from HSS. This information retrieval is needed only if necessary information to execute the EAP authentication is not already available in 3GPP AAA Server. To identify the user the *username* part of the provided NAI identity is utilised.

4 Subscribers WLAN related profile is retrieved from HSS. This profile includes e.g. the authorisation information and permanent identity of the user. Retrieval is needed only if subscriber profile information is not already available in 3GPP AAA Server.

5 If the EAP authentication and authorisation was successful, then 3GPP AAA Server sends Access Accept message to WLAN. In this message 3GPP AAA Server includes EAP Success message, keying material derived from the EAP authentication as well as connection authorisation information (e.g. NAS Filter Rule or Tunnelling attributes) to the WLAN.
WLAN stores the keying material and authorisation information to be used in communication with the authenticated WLAN UE.

NOTE: In the roaming case, authorisation information is passed from 3GPP AAA Server to 3GPP AAA Proxy in the form of Local service identifiers (see Section 6.5)

6 WLAN informs the WLAN UE about the successful authentication and authorisation with the EAP Success message.

7 3GPP AAA server registers the WLAN users 3GPP AAA Server to the HSS. In registration messages the subscriber is identified by his permanent identity. This registration is needed only if the subscriber is not already registered to this 3GPP AAA Server.

************************** End of Changes *****************************

3GPP TSG-SA WG2 Meeting #40
Sophia Antipolis, France, 17-21 May 2004

Tdoc ⌘S2-041851

CR-Form-v7

CHANGE REQUEST

⌘	**23.234**	**CR**	**044**	⌘**rev**	**1**	⌘	Current version:	**6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME □ Radio Access Network □ Core Network ☒

Title:	⌘	Correction of Wd reference point requirements		
Source:	⌘	SA2 (Nortel Networks)		
Work item code:	⌘	WLAN	***Date:*** ⌘	18/05/2004
Category:	⌘	**F**	***Release:*** ⌘	Rel-6
		Use one of the following categories: ***F** (correction)* ***A** (corresponds to a correction in an earlier release)* ***B** (addition of feature),* ***C** (functional modification of feature)* ***D** (editorial modification)* Detailed explanations of the above categories can be found in 3GPP TR 21.900.		*Use one of the following releases:* *2 (GSM Phase 2)* *R96 (Release 1996)* *R97 (Release 1997)* *R98 (Release 1998)* *R99 (Release 1999)* *Rel-4 (Release 4)* *Rel-5 (Release 5)* *Rel-6 (Release 6)*

Reason for change:	⌘	Tunnel establishment is end-to-end and independent of WLAN Access Authorisation. However the TS indicates that the Wd reference point between AAA server and AAA proxy carries information related to tunnel establishement, tunnel data integrity and encryption. This is only true in the case in which the PDG is located in the VPLMN.
Summary of change:	⌘	Clarify that the requirement for the Wd reference point to carry this information applies only in the case that that the PDG is in the VPLMN.
Consequences if not approved:	⌘	Mis-leading specification.

Clauses affected:	⌘	6.3.11				
		Y	**N**			
Other specs affected:	⌘		X	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

************************** Start of Changes ******************************

6.3.11 Wd reference point

6.3.11.1 General description

The Wd reference point connects the 3GPP AAA Proxy, possibly via intermediate networks, to the 3GPP AAA Server. The prime purpose of the protocols crossing this reference point is to transport authentication, authorization and related information in a secure manner.

EAP authentication shall be transported over the Wd reference point.

6.3.11.2 Functionality

The functionality of the reference point is to transport AAA messages including:

- Carrying data for authentication signalling between 3GPP AAA Proxy and 3GPP AAA Server
- Carrying data for authorization signalling between 3GPP AAA Proxy and 3GPP AAA Server
- Carrying charging signalling per WLAN user
- Carrying keying data for the purpose of radio interface integrity protection and encryption
- Carrying authentication data for the purpose of tunnel establishment, tunnel data authentication and encryption, for the case in which the PDG is in the VPLMN.
- Used for purging a user from the WLAN access for immediate service termination
- Enabling the identification of the operator networks amongst which the roaming occurs

************************** Next Change ******************************

3GPP TSG-SA WG2 Meeting #40
Sophia Antipolis, France, 17-21 May 2004

Tdoc ⌘S2-041852

CR-Form-v7

CHANGE REQUEST

⌘	**23.234**	**CR**	**045**	⌘**rev**	**1**	⌘	Current version:	**6.0.0**	⌘

For ***HELP*** *on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME □ Radio Access Network □ Core Network ☒

Title:	⌘	Clarification of Wm reference point requirements		
Source:	⌘	SA2 (Nortel Networks, Ericsson, Nokia)		
Work item code:	⌘	WLAN	***Date:*** ⌘	18/05/2004
Category:	⌘	F	***Release:*** ⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Description of the Wm reference point contains an unclear reference to 'service authentication' and 'service authorisation', which should be 'user authentication' and 'user authorisation'.
Summary of change:	⌘	The sentences are clarified
Consequences if not approved:	⌘	Incorrect specification

Clauses affected:	⌘	6.3.10				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

************************* Start of Changes *****************************

6.3.10 Wm reference point

The Wm reference point applies to scenario-3.

This reference point is located between 3GPP AAA Server and Packet Data Gateway. The functionality of this reference point is to enable:

- The 3GPP AAA Server to retrieve tunneling attributes and WLAN UE's IP configuration parameters from/via Packet Data Gateway.
- Carrying messages between PDG and AAA Server in support of~~for~~ ~~service~~ the user authentication exchange which takes place between WLAN UE and 3GPP AAA server.
- Carrying messages for ~~service~~ user authorization between PDG and 3GPP AAA server.
- Carrying authentication data for the purpose of tunnel establishment, tunnel data authentication and encryption.

************************* End of changes *****************************

3GPP TSG-SA2 Meeting #40 **Tdoc ⌘S2-042283**
Sophia Antipolis, France, 17th – 21st May 2004

CR-Form-v7

CHANGE REQUEST

⌘ **23.234** **CR** **047** ⌘**rev** **2** ⌘ Current version: **6.0.0** ⌘

For ***HELP*** *on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME □ Radio Access Network □ Core Network ☒

Title:	⌘	Re-authentication		
Source:	⌘	SA2 (Samsung)		
Work item code:	⌘	WLAN	***Date:*** ⌘	21/05/04
Category:	⌘	***F***	***Release:*** ⌘	*Rel-6*

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	The section about re-authentication has has out-dated information and 'FFS'. Also wrong information exist about re-authetication during redirection.
Summary of change:	⌘	Add clarification for fast re-authentication when subsequent authentication happens.
Consequences if not approved:	⌘	The section will contain 'FFS'

Clauses affected:	⌘	7.9.1, 7.9.2			
		Y	**N**		
Other specs affected:	⌘		**X**	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

******** FIRST MODIFIED SECTION ********

7.9.1 Redirection

In the above procedures, the WLAN UE may not be authorised to access the requested W-APN through the selected PDG. This may occur for the following reasons:

(i) The requested W-APN is not supported by the network

(ii) The user is not subscribed to the requested W-APN

(iii) The PDG is in the VPLMN and the user's subscription indicates that VPLMN access is not allowed for the requested W-APN

(iv) The operator does not wish to include all PDG addresses in DNS and so (for example) all initial requests are handled by a default PDG which may not be the correct PDG for the requested W-APN

(v) The user has not supplied an explicit requested W-APN. This is treated as a request for the first appropriate subscribed W-APN, or for a network default W-APN (if a wildcard W-APN is included in the subscription), as per 23.060 Annex A.

In cases (i), (ii) and (iii), the request is simply rejected. In case (iii), the WLAN UE may attempt tunnel establishment to the HPLMN as described in Section 7.8.

In cases (iv) and (v) above, the AAA Server may determine that the user is authorised to access the W-APN through a different PDG. The IP address of the alternative PDG is then returned to the WLAN UE in the rejection message from PDG to WLAN UE. In this case the WLAN UE shall attempt a new tunnel establishment request to the provided PDG address.

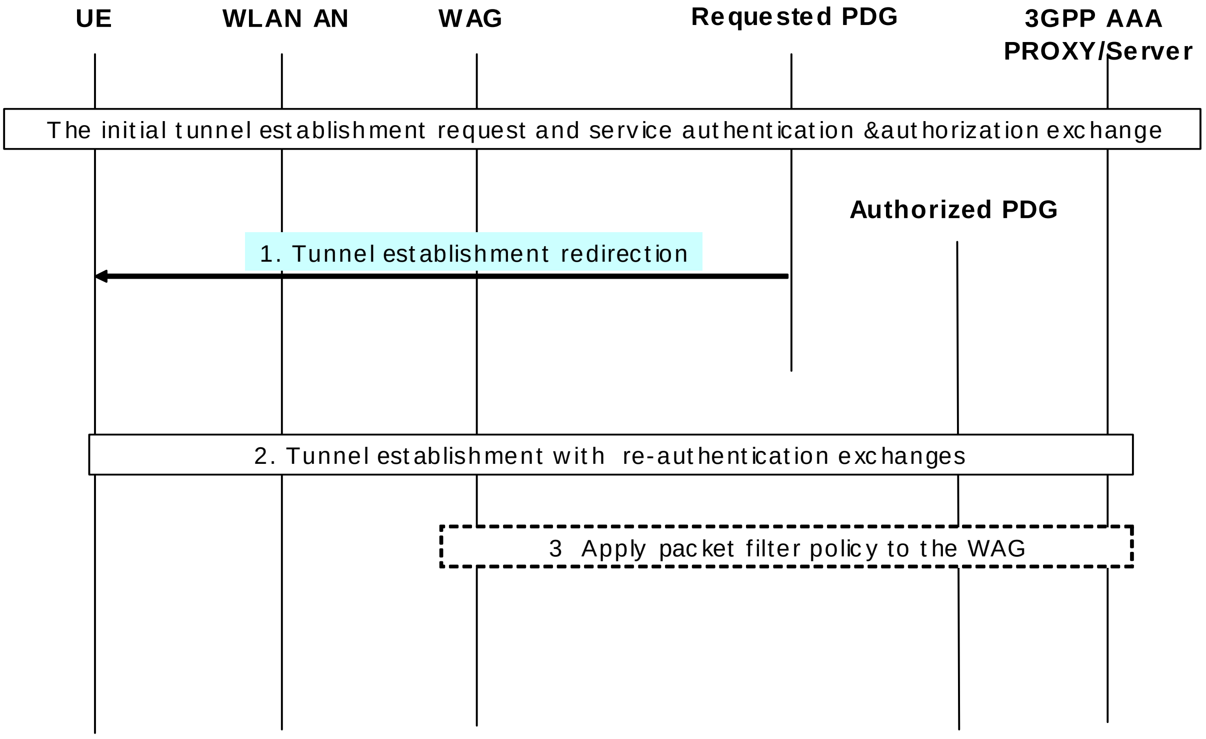

UE
WLAN AN
WAG
Requested PDG
3GPP AAA PROXY/Server
The initial tunnel establishment request and service authentication &authorization exchange
Authorized PDG
1. Tunnel establishment redirection
2. Tunnel establishment with re-authentication exchanges
3 Apply packet filter policy to the WAG

Figure 7.11: Message flow of the tunnel establishment with redirection

During the step 2.3/3.3 in the procedure of clause 7.9, the 3GPP AAA Server authorizes the service to the WLAN UE, and sends the authorization information to the requested PDG. If requested PDG is not authorized to provide the service then the AAA server sends a new PDG (Authorized PDG) address and the authorized W-APN, then the following steps performed:

1. The requested PDG sends tunnel redirection request to the UE with service authorization information (authorized PDG address~~,~~ and authorized W-APN~~ and the re-authentication parameters provided by the AAA server~~).

2. The WLAN UE sends an end-to-end tunnel establishment request to the Authorized PDG. Then end-to-end tunnel establishment begins between the Authorized PDG and the WLAN UE. A full or fast re-authentication method should be used during this tunnel establishment.

3. The Authorized PDG provides filtering information to the WAG as it is specified in clause 7.9.

7.9.2 Subsequent authentication

In the case that the user attempts a subsequent tunnel establishment to a different PDG, it should be possible to avoid repeating the full authentication process and to perform fast re-authentication. ~~(for example, a shorter re-authentication process should be used). This is ffs in Stage 3 work~~.Fast re-authentication is an optional feature and its activation is performed in the home operator's network.

******** END OF CHANGES ********

3GPP TSG SA SA2 Meeting #40
Sophia Antipolis, France, 17-21 May 2004

S2-042234

CR-Form-v7

CHANGE REQUEST

⌘ **23.234 CR 048** ⌘**rev 3** ⌘ Current version: **6.0.0** ⌘

For ***HELP*** *on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME □ Radio Access Network □ Core Network ☒

Title: ⌘	Alignment with 3GPP IMS architecture: SLF usage in Wx to locate the HSS		
Source: ⌘	SA2 (Ericsson)		
Work item code: ⌘	WLAN	***Date:*** ⌘	21/05/2004
Category: ⌘	F	***Release:*** ⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change: ⌘	3GPP AAA Server communicates to the HSS over the Wx reference point. However, when there multiple separately addressable HSS's, the 3GPP AAA Server does not know the HSS where the user is subcribed.
Summary of change: ⌘	It has been re-used the SLF concept defined in IMS to locate the HSS where the user is subcribed in an HSS configuration of multiple addressable HSS's.
Consequences if not approved: ⌘	The 3GPP AAA Server can not locate the HSS where the user is subscribed

Clauses affected: ⌘	2, 3.2, 5.1, 6.1.1, 6.1.2, 6.2.x (new), 6.3.x (new), 7.x (new)				
	Y	**N**			
Other specs Affected: ⌘	**X**		Other core specifications	⌘	29.234
		X	Test specifications		
		X	O&M Specifications		
Other comments: ⌘	The updated figures in this CR is inline with CR 30r5 (S2-042233) that also updateds the same figures.				

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

****** First modified section ******

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TS 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.101: "Service principles".

[3] 3GPP TR 22.934: "Feasibility study on 3GPP system to WLAN interworking".

[4] 3GPP TS 23.002: "Network architecture".

[5] 3GPP TS 23.003: "Numbering, addressing and identification".

[6] 3GPP TS 23.040: “Technical Realisation of the Short Message Service (SMS)”

[7] 3GPP TS 23.060: "GPRS; Service description".

[8] 3GPP TR 23.934: "3GPP system to WLAN Interworking; Functional and architectural definition".

[9] 3GPP TS 24.234: "3GPP System to WLAN Interworking; UE to Network protocols; Stage 3".

[10] 3GPP TS 29.002: "Mobile Application Part (MAP) specification".

[11] 3GPP TS 29.329: " Sh Interface based on the Diameter protocol; Protocol details".

[12] 3GPP TS 31.102: "Characteristics of the USIM Application."

[13] 3GPP TS 32.225: "Telecommunication management; Charging management; Charging data description for the IP Multimedia Subsystem (IMS)."

[14] 3GPP TS 33.234: "WLAN Interworking Security."

[15] 3GPP TR 23.825: "Overall Architecture Aspects of IP Flow Based Bearer Level Charging"

[16] RFC2284: "PPP Extensible Authentication Protocol (EAP)"

[17] RFC 2486: "The Network Access Identifier"

[18] J. Caron, "DNS Based Roaming", http://www.ietf.org/internet-drafts/draft-caron-dns-based-roaming-00.txt, April 2002, (work in progress)

[19] IEEE Std 802.1X-2001 IEEE Standard for Local and metropolitan area networks— Port-Based Network Access Control

[20] IETF Internet-Draft: "Network Discovery and Selection within the EAP Framework". draft-adrangi-eap-network-discovery-and-selection-010, work in progress.

[21] IEEE Std 802.11-1999, Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, IEEE, Sep. 1999.

[22] IETF Internet-Draft: “EAP AKA Authentication” draft-arkko-pppext-eap-aka-11 (October 2003).

[23] IETF Internet-Draft: “EAP SIM Authentication” draft-haverinen-pppext-eap-sim-12 (October 2003).

[24] 3GPP TS 23.228: " IP Multimedia Subsystem (IMS); Stage 2".

****** Next modified section ******

3.2 Symbols

For the purposes of the present document the following symbols apply:

D'	Reference point between a pre-R6 HSS/HLR and a 3GPP AAA Server
Dw	Reference point between a 3GPP AAA Server and an SLF
Gr'	Reference point between a pre-R6 HSS/HLR and a 3GPP AAA Server
Wa	Reference point between a WLAN Access Network and a 3GPP AAA Server/Proxy (charging and control signalling)
Wd	Reference point between a 3GPP AAA Proxy and a 3GPP AAA Server (charging and control signalling)
Wf	Reference point between a CGw/CCF and a 3GPP AAA Server/Proxy
Wg	Reference point between a 3GPP AAA Proxy and WAG
Wi	Reference point between a Packet Data Gateway and an external IP Network
Wm	Reference point between a Packet Data Gateway and a 3GPP AAA Server
Wn	Reference point between a WLAN Access Network and a WLAN Access Gateway
Wp	Reference point between a WLAN Access Gateway and a Packet Data Gateway
Wo	Reference point between a 3GPP AAA Server and an OCS
Wu	Reference point between a WLAN UE and a Packet Data Gateway
Wx	Reference point between an HSS and a 3GPP AAA Server

****** Next modified section ******

5 High-level Requirements and Principles

5.1 Access Control Requirements

The following functional requirements have been identified:

- Legacy WLAN terminals should be supported. However software upgrades may be required for e.g. security reasons.
- Minimal impact on the user equipment, i.e. client software.
- Minimal impact on existing WLAN networks.
- The need for operators to administer and maintain end user software shall be minimized.
- Existing SIM and USIM shall be supported.
- Authentication shall rely on (U)SIM based authentication mechanisms.
- R6 USIM may include new functionality if necessary e.g. in order to improve privacy.
- Changes in the HSS/HLR/AuC shall be minimized.
- SLF node shall be used in the same way as defined in 3GPP TS 23.228 [24] to find the address of the HSS that holds the subscriber data for a given user identity when multiple and separately addressable HSSs have been deployed by the network operator.
- Methods for key distribution to the WLAN access network shall be supported.
- The WLAN connection established for a 3GPP subscriber shall have no impact to the capabilities of having simultaneous PS and CS connections for the same subscriber.
- WLAN Access Authorization shall occur upon the success of the authentication procedure. It shall take into account the user's subscription profile and optionally information about the WLAN AN, such as WLAN AN operator name, WLAN AN location information (e.g., country, telephone area code, city), WLAN AN throughput (e.g., maximum and minimum bandwidth guarantees for both ingress and egress traffic). This information is used to enable use-case scenarios like location based authentication/authorization, location based billing / customer care, and location based service offerings.
- It shall be possible to indicate to the user of the results of authorization requests.
- Results of WLAN Access Authorization requests shall be indicated to the WLAN, so that the WLAN can take appropriate action.
- The WLAN Access Authorization mechanism shall be able to inform the user and WLAN immediately of any change in service provision.
- This TS proposes solutions for operators who want to interwork their WLAN with an existing pre-R6 HLR/HSS.

Additional access control requirements for scenario 3:

- Service Authorization shall occur after the WLAN Access Authentication/Authorization procedure.
- Service based policy control shall be possible for the services authorized for the user.
- Access to 3GPP PS based services shall be provided via WLAN. The interworking architecture shall be able to support all 3GPP PS based services.
- Access to PS based services normally provided by the 3GPP PS Core Network shall be provided via WLAN. WLAN access to these services shall support the same features as those supported via the 3GPP PS Core Network according to operator choice, e.g. private addressing schemes, external address allocation, secure tunneling to private external network. Quality of Service shall be supported when accessing these services via WLAN, although some limitations may exist because of the WLAN AN.
- A scenario 3 WLAN inter-working system shall be able to support WLAN UEs operating in scenario 2, e.g. according to subscription.
- A Scenario3 capable user should be able to choose between a scenario2 type of internet access (direct access through local network) or a scenario3 type of access to internet (through the PLMN), when the network allows it.
- When the WLAN inter-working system does not support access to 3GPP PS based services, the WLAN UE shall be able to detect it.

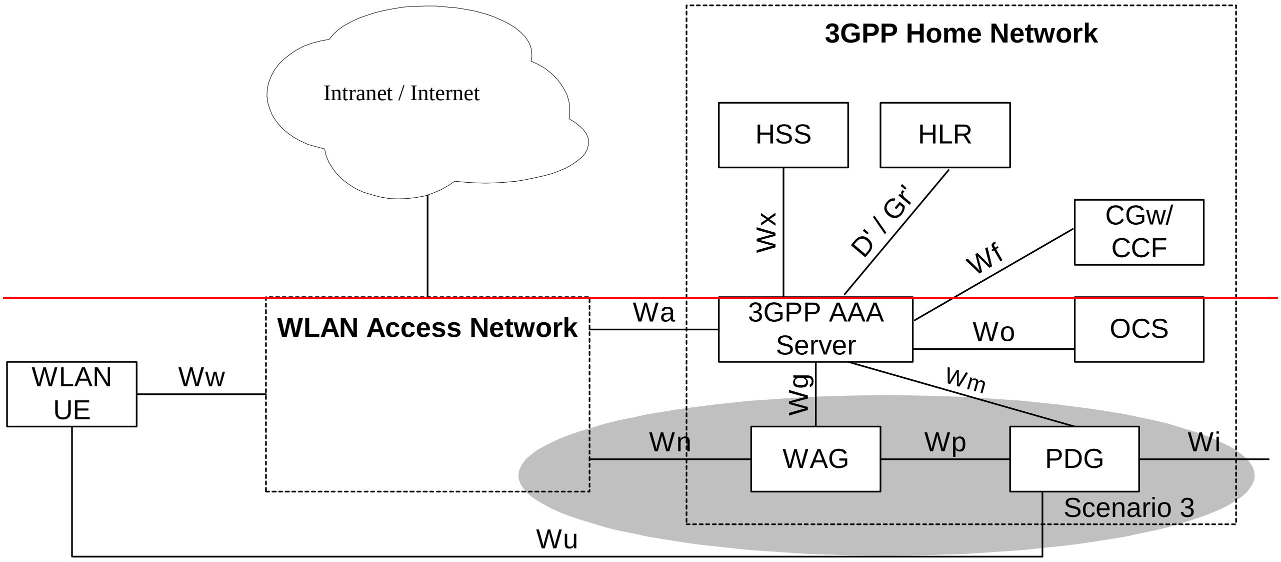
- A scenario 3 WLAN inter-working system shall be able to mandate all flows for 3G PS based services to be routed to the HPLMN or the VPLMN, e.g. according to subscription. This routing enforcement shall not rely on the WLAN UE client.

Note: This may mandate additional functionality existing in the WLAN AN

The technical solution for access control to External IP networks from WLAN shall be decoupled from WLAN Access Control.

****** Next modified section ******

6.1.1 Non Roaming WLAN Inter-working Reference Model



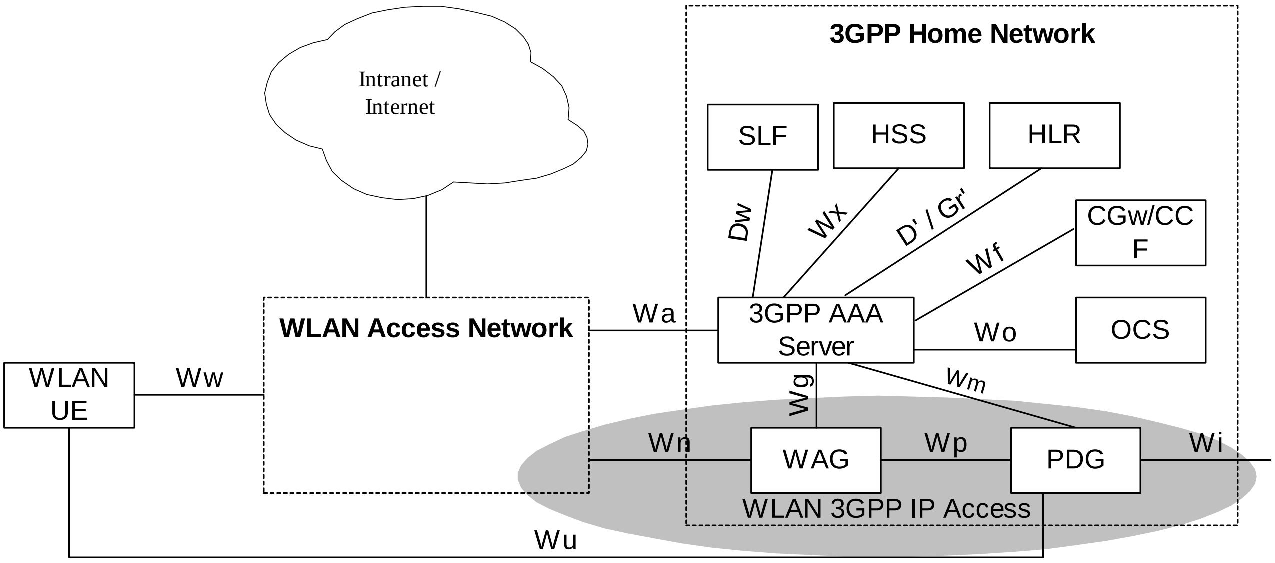


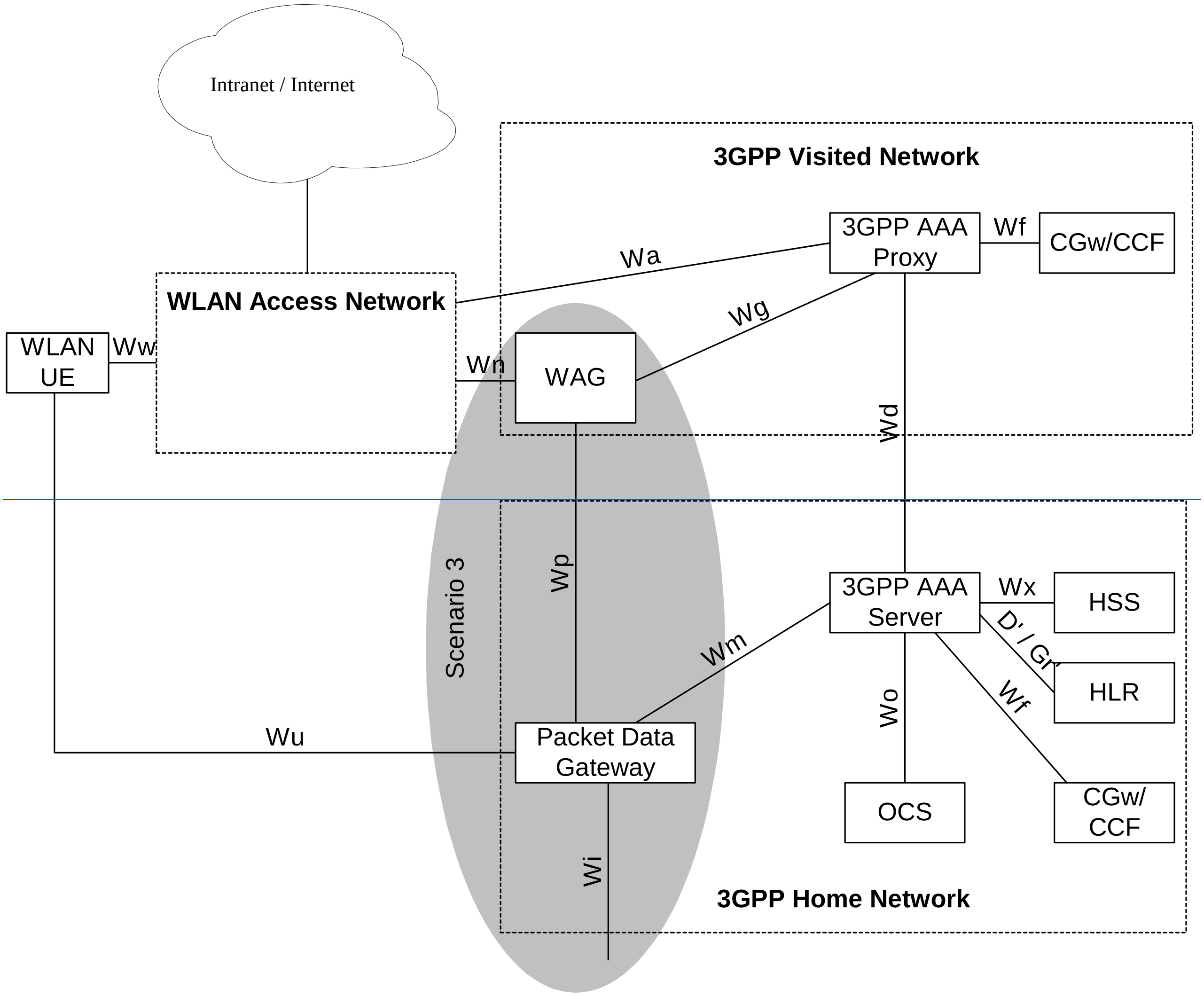
Figure 6.1 Non Roaming Reference Model. The shaded area refers to scenario 3 functionality

6.1.2 Roaming WLAN Inter-working Reference Model

The home network is responsible for access control. Charging records can be generated in the visited and/or the home 3GPP networks. The Wx and Wo reference points are intra-operator. The home 3GPP network interfaces to other 3GPP networks via the inter-operator Wd reference point.

The 3GPP AAA proxy relays access control signalling and accounting information to the home 3GPP AAA Server using the Wd reference point.

It can also issue charging records to the visited network CGw/CCF when required. The 3GPP network interfaces to WLAN Access Networks via the Wa reference point.



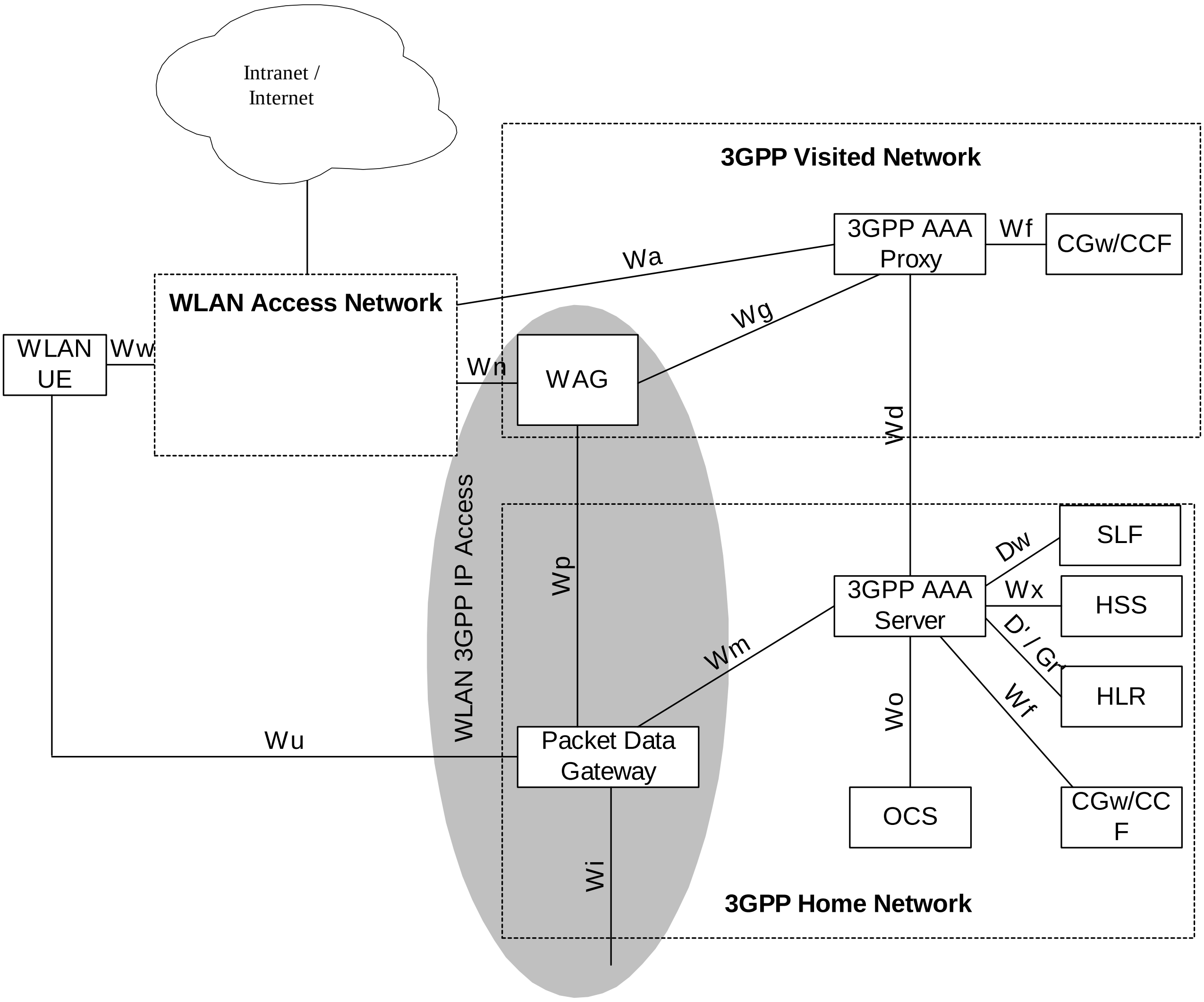
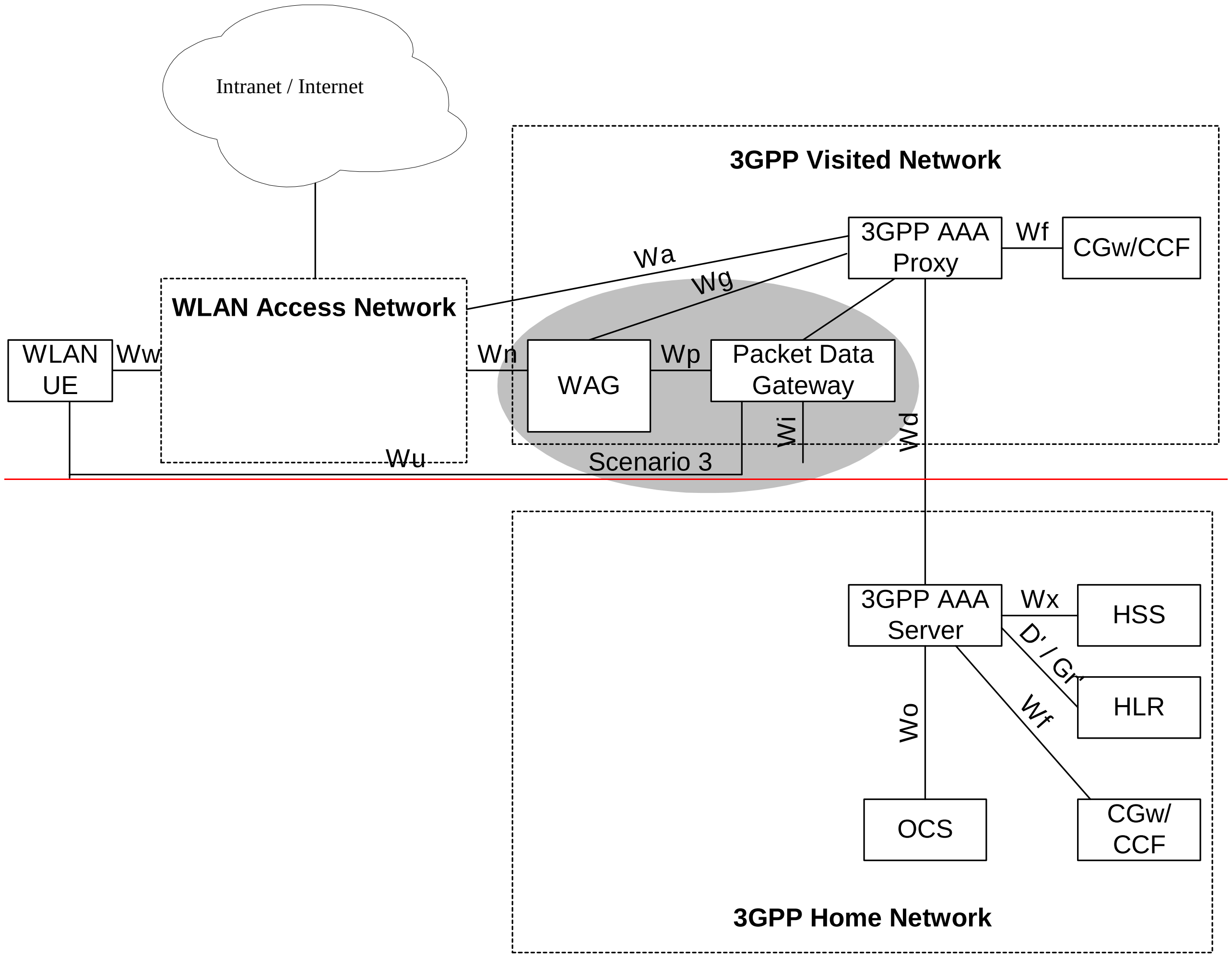


Figure 6.2a. Roaming Reference Model- 3GPP PS based services provided via the 3GPP Home Network (the shaded area refers to scenario 3 functionality)


Intranet / Internet
3GPP Visited Network
3GPP AAA Proxy
Wf
CGw/CCF
Wa
Wg
WLAN Access Network
WLAN UE
Ww
Wn
WAG
Wp
Packet Data Gateway
Wi
Wd
Wu
Scenario 3
3GPP AAA Server
Wx
HSS
D' / Gr'
HLR
Wf
Wo
OCS
CGw/ CCF
3GPP Home Network

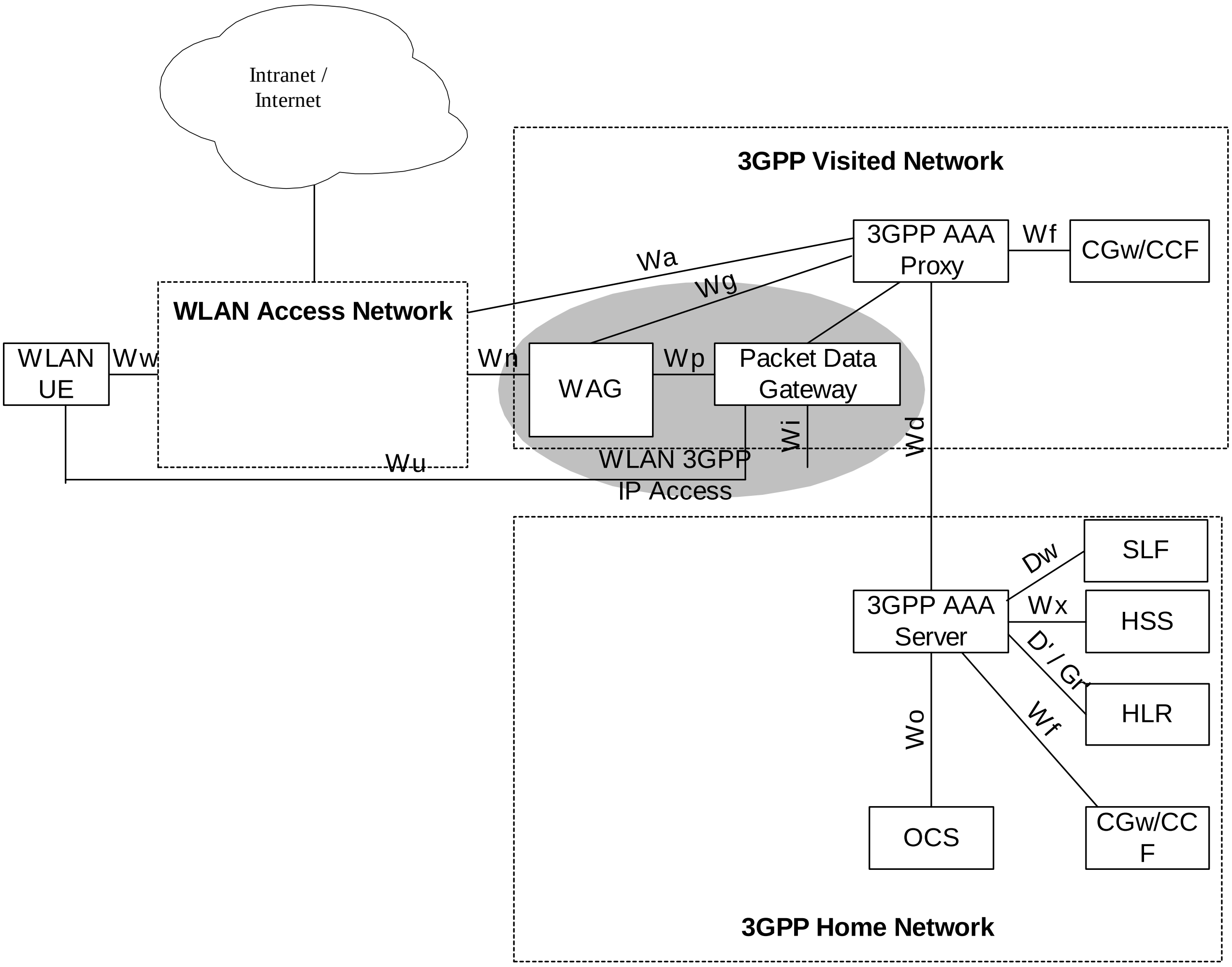


Figure 6.2b. Roaming Reference Model- 3GPP PS based services provided via the 3GPP Visited Network (the shaded area refers to scenario 3 functionality)

****** Next modified section ******

6.2.x Subscription Locator Function (SLF)

The SLF is located within the 3GPP subscriber's home network and enables the 3GPP AAA Server to find the address of the HSS which holds the subscriber data for a given user identity in a configuration with multiple separately addressable HSS'es. The SLF should be used in the same way for WLAN as for IMS, which is specified in 3GPP TS 23.228 [24].

****** Next modified section ******

6.3.x Dw reference point

This reference point is between the 3GPP AAA Server and the SLF. The prime purpose of the protocol(s) crossing this reference point is to enable the 3GPP AAA Server to find the address of the HSS which holds the subscriber data for a given user identity in a configuration with multiple separately addressable HSS'es.

****** Next modified section ******

7.x User identity to HSS resolution

7.x.1 General

This section describes the resolution mechanism, which enables the 3GPP AAA Server to find the address of the HSS, that holds the subscriber data for a given user identity when multiple and separately addressable HSSs have been deployed by the network operato This resolution mechanism is not required in networks that utilise a single HSS. An example for a single HSS solution is a server fa architecture. The NAI will be used as user identifier towards the SLF.

The subscription locator is accessed via the Dw reference point. The Dw reference point is the standard interface between the 3GPP Server and the SLF. The synchronisation between the SLF and the different HSSs is an O&M issue.

The subscription locator is already defined in 3GPP TS 23.228 [24] for Cx and Sh interfaces.

The Dw interface provides:

- an operation to query the subscription locator from 3GPP AAA Server
- a response to provide the HSS name towards 3GPP AAA Server.

By sending the Dw-operation DW_SLF_QUERY the 3GPP AAA Server indicates a user identity of which it is looking for an HSS. the Dw-operation DW_SLF_RESP, the SLF responds with the HSS address. The 3GPP AAA Server may optionally store the HSS address for a given subscriber so subsequent queries to the SLF are not needed.

Subclause 7.x.2 presents an example of the session flow when the 3GPP AAA Server needs to query the SLF.

7.x.2 SLF query

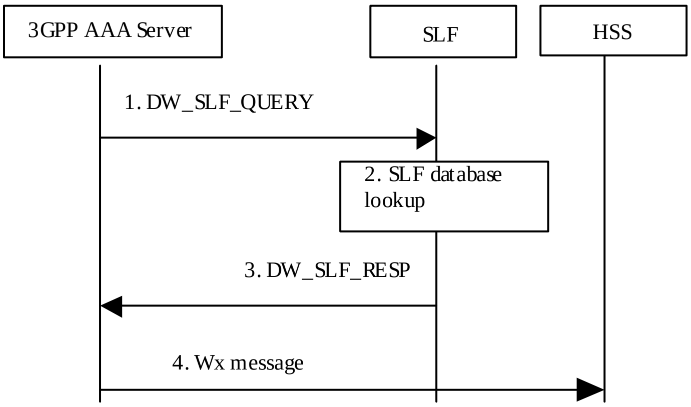


Figure x.x: Query through SLF

1. 3GPP AAA Server detects that it requires the user profile, the registration or new authentication vectors for a given 3GPP subscriber, so has to query for the location of the user's subscription data. The 3GPP AAA Server sends a DW_SLF_QUERY to the SLF and includes as parameter the user identity of the subscriber.

2. The SLF looks up its database for the queried user identity.

3. The SLF answers with the HSS address in which the user's subscription data can be found.

4. The 3GPP AAA Server can proceed by querying the appropriate HSS by Wx protocol.

3GPP TSG SA SA2 Meeting #40
Sophia Antipolis, France, 17-21 May 2004

S2-042235

CR-Form-v7

CHANGE REQUEST

⌘ **23.234**	**CR**	**052**	⌘ **rev**	**2** ⌘	Current version: **6.0.0** ⌘

For ***HELP*** *on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network ☒

Title:	⌘	Removal of WLAN UE classes		
Source:	⌘	SA2 (Ericsson, Nokia, RIM)		
Work item code:	⌘	WLAN	***Date:*** ⌘	20/05/2004
Category:	⌘	**F**	***Release:*** ⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	The WLAN UE classed is currently defined in TS 23.234. However, these classes are only defined but never used anywhere in any specifiction. Also, currently the classes are not forseen how they should be used. Therefore, to clean up the TS and avoid confusions in other groups, it is suggested that the WLAN UE classes are removed.
Summary of change:	⌘	Remove section 6.2.1.1 WLAN UE classes and add clarification in section 6.2.1
Consequences if not approved:	⌘	Unclear TS with definition of WLAN UE classes that are not used.

Clauses affected:	⌘	6.2.1, 6.2.1.1				
		Y	**N**			
Other specs Affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

****** First change ******

6.2.1 WLAN UE

A WLAN UE is the UE (equipped with UICC card including (U)SIM) utilized by a 3GPP subscriber to access the WLAN network for 3GPP interworking purpose. The WLAN UE may be capable of WLAN access only, or it may be capable of both WLAN and 3GPP radio access. Some WLAN UE's may be capable of simultaneous access to both WLAN and 3GPP radio access. A WLAN UE may include terminal types whose configuration (e.g. interface to a UICC), operation and software environment are not under the exclusive control of the 3GPP system operator, such as a laptop computer or PDA with a WLAN card, UICC card reader and suitable software applications.

****** Second change ******

6.2.1.1 ~~WLAN UE classes~~Void

~~According to its capability, a WLAN UE is categorized into three classes.~~

~~Class WA WLAN UE: This class of a WLAN UE has both 3GPP and WLAN radio interfaces. The WLAN UE can be attached to both WLAN and 3GPP systems at the same time, when an interworking WLAN is available. Also it supports simultaneous access to both WLAN and 3GPP cellular network by activating both radio interfaces.~~

~~Class WB WLAN UE: This class of a WLAN UE has both 3GPP and WLAN radio interfaces. But it does not support simultaneous access to both WLAN and 3GPP cellular network because it can operate only one radio interface at a time.~~

~~Class WC WLAN UE: This class of a WLAN UE has only a WLAN radio interface. It is capable of WLAN attach and WLAN access only, when an interworking WLAN is available.~~

3GPP TSG SA SA2 Meeting #40
Sophia Antipolis, France, 17-21 May 2004

S2-042319

CR-Form-v7

CHANGE REQUEST

⌘	**23.234**	**CR**	**053**	⌘**rev**	**1**	⌘	Current version:	**6.0.0**	⌘

For ***HELP*** *on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME □ Radio Access Network □ Core Network ☒

Title:	⌘	Merge of approved CR's in TS 23.234, Annex F		
Source:	⌘	SA2 (Ericsson)		
Work item code:	⌘	WLAN	***Date:*** ⌘	20/05/2004
Category:	⌘	F	***Release:*** ⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Merge of CR no 9r3, 26r4, 40r2, 42r1 towards TS 23.234.
Summary of change:	⌘	Merge of CR no 9r3, 26r4, 40r2, 42r1 towards TS 23.234.
Consequences if not approved:	⌘	Agreed CR's cannot be implemented correctly.

Clauses affected:	⌘	F1, F2, F3, F4, F5			
		Y	**N**		
Other specs affected:	⌘		**X**	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

****** First change ******

6.2.6 Packet Data Gateway

The Packet Data Gateway applies to scenario-3.

3GPP PS based services (Scenario 3) are accessed via a Packet Data Gateway. 3GPP PS based services may be accessed via a Packet Data Gateway in the user's Home Network or a PDG in the selected VPLMN. The process of authorisation and service selection (e.g. W-APN selection) and subscription checking determines whether a service shall be provided by the home network or by the visited network. The resolution of the IP address of the Packet Data Gateway providing access to the selected service will be performed in the PLMN functioning as the home network (in the VPLMN or HPLMN).

Successful activation of a selected service results in:

- Determination of the Packet Data Gateway IP address used by the WLAN UE;
- Allocation of a WLAN UE's remote IP address to the WLAN UE (if one is not already allocated);
- Registration of the WLAN UE's local IP address with the Packet Data Gateway and binding of this address with the WLAN UE's remote IP address.

The Packet Data Gateway:

- Contains routeing information for WLAN-3G connected users;
- Routes the packet data received from/sent to the PDN to/from the WLAN-3G connected user;
- Performs address translation and mapping;
- Performs de-capsulation and encapsulation;
- accepts or rejects the requested W-APN according to the decision made by the 3GPP AAA Server;
- redirects the tunnel establishment request towards another PDG if this is indicated to be done by the 3GPP AAA Server

Allows allocation of the WLAN UE's remote IP address;

- Relays the WLAN UE's remote IP address allocated by an external IP network to the WLAN UE, when external IP network address allocation is used.
- Performs registration of the WLAN UE's local IP address and binding of this address with the WLAN UE's remote IP address;
- Provides procedures for unbinding a WLAN UE's local IP address with the WLAN UE's remote IP address;
- Provides procedures for authentication and prevention of hijacking (i.e. ensuring the validity of the WLAN UE initiating any binding of the WLAN UE's local IP address with the WLAN UE's remote IP address, unbinding etc.)
- May filter out unauthorised or unsolicited traffic with packet filtering functions. All types of message screening are left to the operators' control, e.g. by use of Internet firewalls.
- Generates per user charging information.
- Generates charging information related to user data traffic for offline and online charging purposes.
- May apply IP flow based bearer level charging [13], e.g. in order to differentiate or suppress WLAN bearer charging for 3GPP PS based services.
- Performs the functions of Service-based Local Policy Enforcement Point (controls the quality of service that is provided to a set of IP flow as defined by a packet classifier, control admission based on policy that is applied to

the IP bearers associated with the flow, and configuration of the packet handling and "gating" functionality in the user plane.)

- Communicates with Policy Decision Function (PDF) to allow service-based local policy and QoS inter-working information to be "pushed" by the PDF or to be requested by the PDG. This communication also provides information to support the following functions in the PDG:
  - Control of Diffserv inter-working;
  - Control of RSVP admission control and inter-working;
  - Control of "gating" function in PDG;
  - WLAN bearer authorization;
  - QoS charging related function.

Annex F describes how PDG functionality can be provided by re-useing existing unmodified GGSN functionality.

****** Second change ******

Annex F (~~informative~~normative): Information on re-using the GGSN to implement the PDG function~~via the Gn' reference point~~

This annex does not introduce new normative requirements for the PDG.

F.1 Introduction

This section provides information on how to re-use existing GGSN deployments to implement the PDG functionality via using a subset of the Gn reference point (denoted here as Gn'). The Gn' reference point provides ~~an optional~~ means where GPRS mobile operators can reuse existing infrastructure and functionality for a user accessing from a WLAN UE. By using this existing standardized ~~standardizing this~~ reference point, interoperability ~~between a decomposed Packet Data Gateways (PDG) and~~ towards the Gateway GPRS Support Nodes (GGSN) is assured. ~~Both the decomposed PDG and the GGSN shall be located in the same PLMN, i.e. HPLMN or VPLMN. The use of Gn' reference point in an operator network is therefore independent of other operators networks. Gn' reference point will provide reuse of GPRS infrastructure. The decomposition of PDG functionality~~ Such a PDG implementation allows ~~to~~ re-use of existing GGSN functionality without upgrading GGSNs. For example, GGSN functions, which are used in this case are:

- Charging Gateway interfaces;
- IP address allocation;
- Authentication in external networks;
- Single access to 3GPP PS domain services.

Traffic Plane Functionality in the GGSN for online and offline service data flow charging (IP ~~bearer~~ flow level bearer charging), introduced in Release 6 may also be re-used ~~(although this function could equally be provided at the PDG)~~.

The following figure depicts a PDG implementation that re-uses GGSN functionality. It shall be noted that only a subset of the GGSN is reused for this purpose.

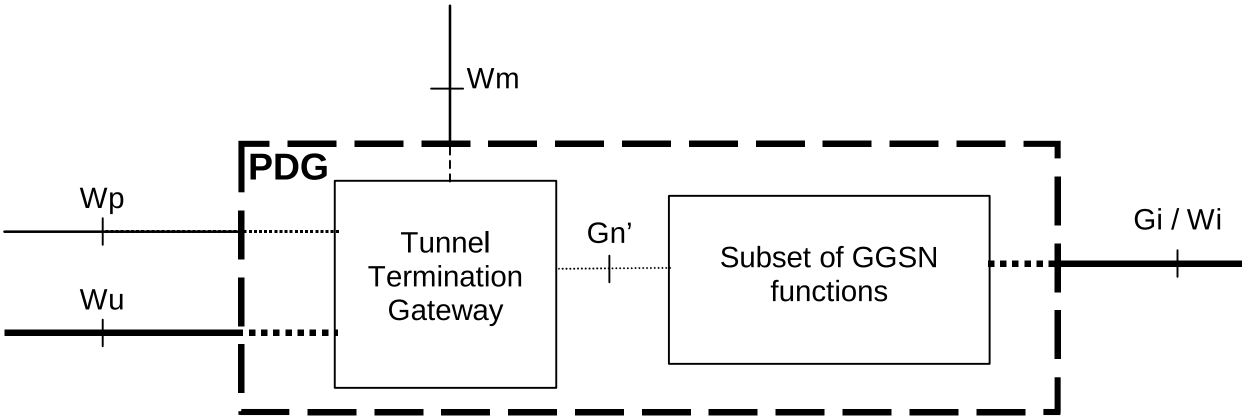


Figure F.1: PDG implementation re-using GGSN functionality

The PDG functionality described in this specification may be implemented using the architecture described above in Figure F.1. In case this implementation is applied, the TTG and GGSN parts of the PDG shall be in the same PLMN. This type of PDG implementation shall remain transparent to the other functional elements of the network.

F.2 Mapping between E2E tunnel and GTP tunnel

The end-to-end tunnel between the WLAN UE and the PDG is setup according to the procedure described in ~~TS 23.234~~ this specification. In a configuration when the Gn' reference point is used, then the end-to-end tunnel setup is terminated by the TTG of the PDG, and ~~with a decomposed PDG, then this procedure triggers~~ the setup of ~~the~~ a GTP tunnel is triggered towards the GGSN part of the PDG. ~~between the decomposed PDG and the GGSN.~~ Each end-to-end tunnel is mapped one-to-one to a GTP tunnel. The GTP tunnel between the ~~decomposed PDG~~ TTG part and the GGSN part of the PDG is established using the two messages Create PDP Context Request and Create PDP Context Response. A GTP tunnel is identified in each node with a TEID (Tunnel End-point Identifier - an integer), an IP address and a UDP port.

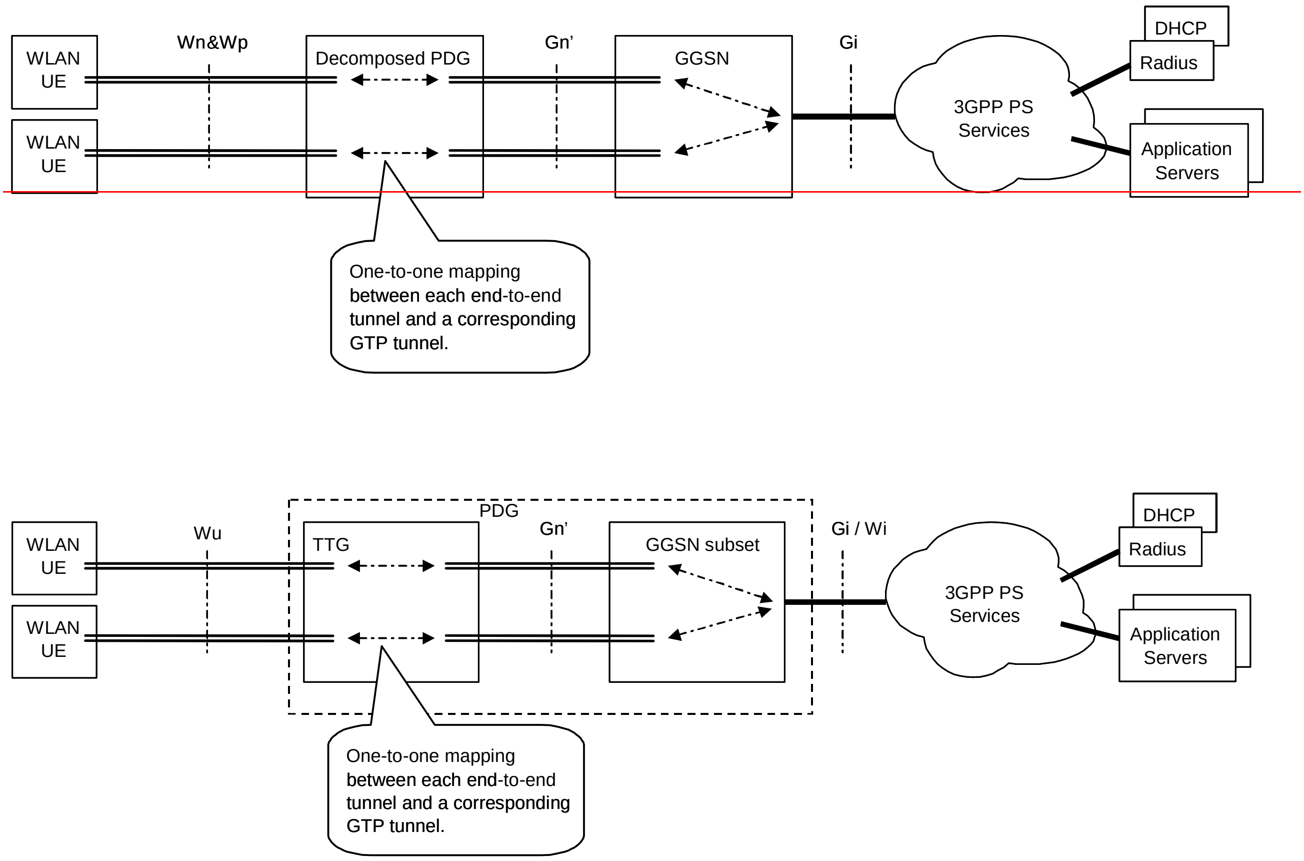


Figure F.2: Mapping between E2E tunnel and GTP tunnel

In GPRS different quality-of-service can be assigned to GTP tunnels. WLAN support of layer 2 QoS is being addressed by the IEEE 802.11e study group. Work specifying the interactions with signalling techniques to support the different quality of service techniques needs to be defined. It is unclear at this time how to have a QoS mapping from IEEE 802.11e to IP and hence to the GTP tunnel.

The W-APN provided over the end-to-end tunnel shall be forwarded in the Create PDP Context Request message to GGSN to select external network e.g. PLMN service network, a corporate intranet or the Internet. Internet access can be provided directly from the WLAN Access Network using ~~scenario 2~~for WLAN Direct IP Access, but of course nothing prevents a PLMN operator from providing Internet access as well via Gi interface using ~~scenario 3~~for WLAN 3GPP IP Access. Some mobile operators might have benefits in using one unified access for all kinds of traffic.

The IMSI of the WLAN UE shall be forwarded to GGSN in the Create PDP Context Request message.

For further details on GTP tunnel management please refer to TS 29.060.

F.3 ~~Interworking procedures over~~ Gn' considerations

Editor's note: ~~The interworking procedures over the Gn' reference point should be specified. It is expected that these procedures are a true subset of the Gn reference point procedures.~~The Gn procedures shall comprise a subset of the Gn reference point procedures. There shall be no enhancements to Gn applied.

F.3.0 General

A minimum set of interworking procedures over the Gn' reference point would include the following messages:

- Create PDP Context Request / Response;

- Update PDP Context Request / Response;
- Delete PDP Context Request / Response;
- Error Indication;
- Version Not Supported;
- GTP payload forwarding (specified in 29.060).

Note: The messages above form a true subset of the Gn reference point messages and procedures.

The TTG must be provided with information, e.g. MCC and MNC of the VPLMN, needed to include the RAI Information Element within the messaging to the GGSN to enable simple position based billing and to enable the HPLMN to restrict certain content to those countries depending on that country's legal requirements.

The assignment of the remote IP address should be done from a pool of IP address belonging to the GGSN/RADIUS server or at least "address range coordinated" with those to enable correct routing on Gi. The End-user-address IE must be provided in the Create PDP Context Request. If address assignment is done by the GGSN/RADIUS, the IE shall be empty in the request message (indicating dynamic address assignment by GGSN/RADIUS), which makes the GGSN/RADIUS assign and return an IP address in the Response message.

To support WLAN UEs, which may use GPRS and WLAN access simultaneously, the NSAPI value to use by TTG need either be a value reserved for TTG or an NSAPI value passed from WLAN UE to TTG. In Existing GPRS, the NSAPI is assigned in the UE and is used to distinguish between a UE´s PDP contexts. The NSAPI is an integer value between 5 and 15.

If a certain charging profile should be applied in GGSN the Charging Characteristics IE may be included. In that case this information needs to be available in the TTG. The Charging Characteristics may be used to give special charging for WLAN in the GGSN. The Charging Characteristic is defined per subscriber and is stored in HLR. For GPRS the Charging Characteristic is sent to SGSN at attach and is forwarded to GGSN at PDP context creation. For WLAN interworking, the TTG may for example get this information from HLR via the 3GPP AAA Server.

F.3.1 Interworking procedure over Gn' - Tunnel establishment procedure

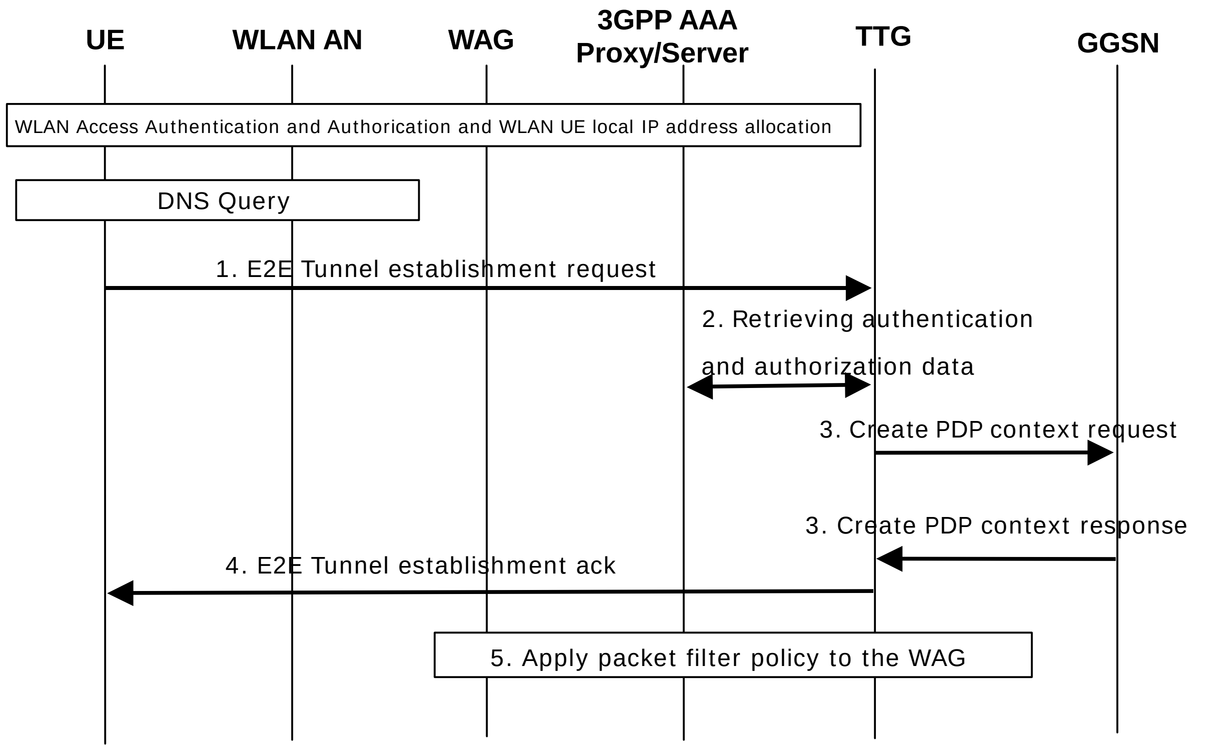

UE
WLAN AN
WAG
3GPP AAA Proxy/Server
TTG
GGSN
WLAN Access Authentication and Authorication and WLAN UE local IP address allocation
DNS Query
1. E2E Tunnel establishment request
2. Retrieving authentication and authorization data
3. Create PDP context request
3. Create PDP context response
4. E2E Tunnel establishment ack
5. Apply packet filter policy to the WAG

Figure F.3.1: Tunnel establishment procedure

1) The UE performs a DNS query to resolve the W-APN and sends E2E tunnel establishment request (W-APN, user identity) to the TTG (see subclause 7.9).

2) The TTG contacts the 3GPP AAA Server in the HPLMN possibly via the AAA proxy for authorization and authentication of the WLAN UE (see subclause 7.9). Additionally, the TTG retrieves the IMSI, MSISDN, and serving network identity from the AAA server.

3) The TTG performs PDP Context Activation procedure towards the GGSN by using Create PDP Context Request message and Create PDP Context Response message (see TS 23.060 [7]).

4) The TTG returns E2E tunnel establishment acknowledgement (remote IP address) to the WLAN UE.

5) The TTG provides filtering information to the WAG (see subclause 7.9).

Editor's Note : it is ffs how the NSAPI value is allocated when the tunnel establishment procedure over Gn' is performed.

F.3.2 Interworking procedure over Gn' - Tunnel disconnection procedure

F.3.2.1 UE initiated tunnel disconnection

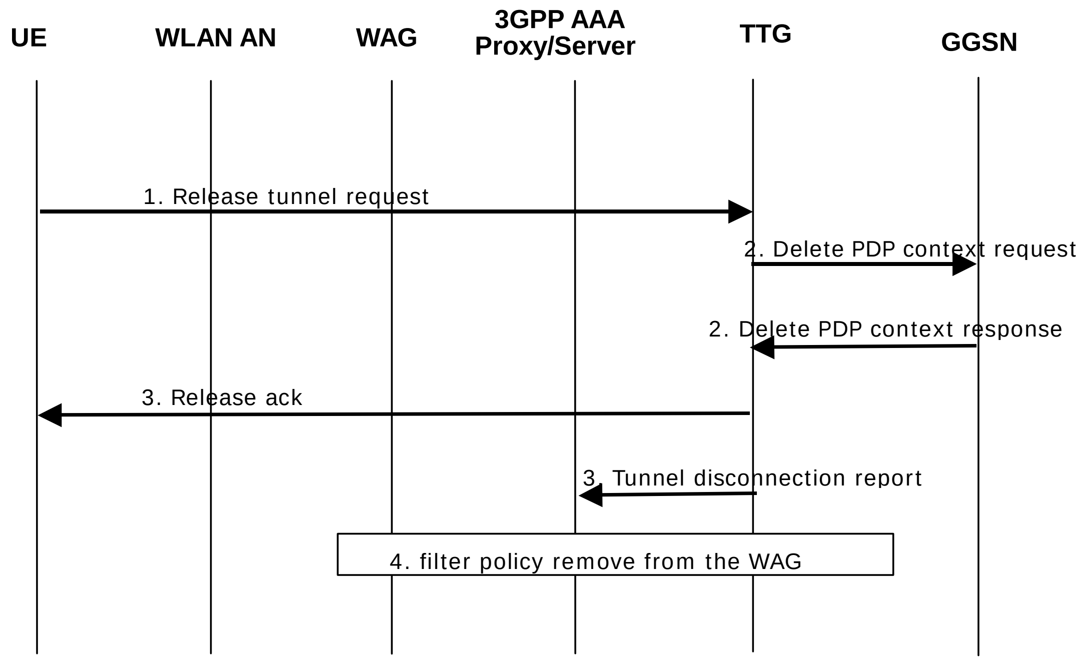

UE
WLAN AN
WAG
3GPP AAA Proxy/Server
TTG
GGSN
1. Release tunnel request
2. Delete PDP context request
2. Delete PDP context response
3. Release ack
3. Tunnel disconnection report
4. filter policy remove from the WAG

Figure F.3.2.1: UE initiated tunnel disconnection procedure

1) The WLAN UE determines to release the tunnel and sends a Release tunnel request to the TTG (see subclause 7.10.1).

2) Upon receiving the Release tunnel request, the TTG performs PDP Context Deactivation procedure towards the GGSN by using Delete PDP Context Request message and Delete PDP Context Response message (see TS 23.060 [7]).

3) The TTG sends a Release acknowledgement to the WLAN UE and Tunnel disconnection report to the 3GPP AAA server (see subclause 7.10.1).

4) Upon receiving the Tunnel disconnection report, the 3GPP AAA server removes the filtering policy from the WAG (see subclause 7.10.1).

F.3.2.2 Network initiated tunnel disconnection

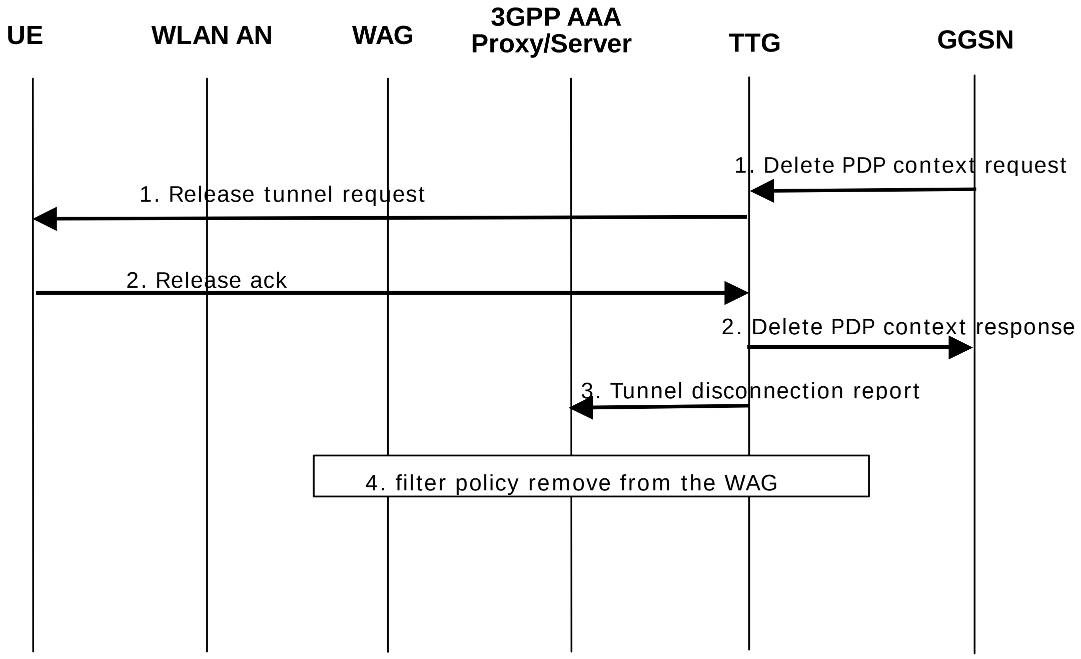

UE
WLAN AN
WAG
3GPP AAA Proxy/Server
TTG
GGSN
1. Delete PDP context request
1. Release tunnel request
2. Release ack
2. Delete PDP context response
3. Tunnel disconnection report
4. filter policy remove from the WAG

Figure F.3.2.2: Network initiated tunnel disconnection procedure

1) The GGSN determines to release the tunnel and sends Delete PDP Context Request message towards the TTG (see TS 23.060 [7]). The TTG then sends a Release tunnel request to the WLAN UE (see subclause 7.10.2).

2) Upon receiving the Release tunnel request, the WLAN UE sends a Release acknowledgement to the TTG (see subclause 7.10.2). The TTG sends a Delete PDP Context Response message to the GGSN (see TS 23.060 [7]).

3) The TTG sends a Tunnel disconnection report to the 3GPP AAA server (see subclause 7.10.2).

4) Upon receiving the Tunnel disconnection report, the 3GPP AAA server removes the filtering policy from the WAG (see subclause 7.10.2).

NOTE: Network initiated tunnel disconnection procedure may also be triggered by the TTG (e.g. request from AAA server).

F.4 Issues to investigate for Gn' reference point

Editor's note: This section is expected to be removed once the investigation on the issues listed here has been concluded.

Some issues that needs to be investigated have been identified~~.~~:

~~- Does the Gn' reference point have any impact on the GGSN? This shall be avoided.~~

~~- The Gn' reference point may introduce packet flows of higher bit rates into the GGSN. Does the current GGSN architecture put any unnecessary capacity constraints on these higher bit rate flows?~~

- GTP requires MSISDN. MSISDN might be a requirement for WLAN for charging or other reasons, but if it doesn't this is an issue. ~~MSISDN is no requirement for WLAN UE's. Is this an issue for GGSN or the GTP protocol?~~

~~- Is the UMTS Bearer Level QoS sufficient to support WLAN traffic?~~

~~- If parallel WLAN and GPRS sessions are allowed (FFS), the GGSN will serve several "SGSN's" i.e. one GPRS SGSN and one WLAN PDG simultaneously. Is his an issue for the GGSN?~~

~~- If Gn' reference point is used, the charging and service specific interfaces in PDG becomes redundant and needs to be handled in the specification in some way. One alternative is to make them conditional, and specify them to be not used if the Gn' reference point is present. Another alternative is to make the Gn' reference point mandatory, whereas the PDG charging and service specific interfaces don't need to be specified at all.~~

~~- As an alternative to reusing GPRS charging specifications and infrastructure, it has been proposed to e.g. co-locate the PDG with the GGSN. A mandatory Gn' reference point can however be a "specification tool", i.e. a way to describe, such an arrangement. This would provide PDG and GGSN co-location with a minimum of impact on existing GGSN specifications. In a PDG & GGSN co-location scenario, the Gn' will stay as a reference point only and never be materialized as an interface. This could be a scenario for future evolvement of the architecture.~~

~~*Editor's note: Functional description of a decomposed PDG is FFS.*~~

F.5 Tunnel Terminating Gateway (TTG) functionality

The functionality of the TTG shall cover all aspects of the PDG that are not covered by the GGSN.

The TTG shall be responsible for allocating NSAPI values before sending Create PDP Context Request towards the GGSN. Although the TTG acts like the SGSN in terms of GTP tunnel establishment, it also manages NSAPI as WLAN UE's proxy for the purpose of leaving the Gn' based PDG transparent to the WLAN UE.

In the case that the network supports simultaneous GPRS and WLAN connections, the TTG shall ensure that the NSAPI values allocated shall not overlap with those used by the UE for GPRS PDP Contexts.

NOTE: This can be achieved by restricting TTG allocated NSAPI values to those which are reserved on the mobile radio layer 3 interface in this case.

The TTG shall reject a tunnel establishment request if all available NSAPI values for the user/GGSN have already been used. However, the TTG should not explicitly indicate the exhaustion of the NSAPI values in such a case.

NOTE: The mechanism above implies that it may not be possible to deploy distinct TTGs providing service for W-APNs which are then served from the same GGSN. That is, for a given user, all tunnels towards W-APNs served from a single GGSN shall be directed to the same TTG.

3GPP TSG-SA2 Meeting #40 **_Tdoc ⌘ S2-042336_**
Sophia Antipolis, France, 17th – 21st May 2004

CR-Form-v7

CHANGE REQUEST

⌘	**23.234**	**CR**	**054**	⌘**rev**	**1**	⌘	Current version:	**6.0.0**	⌘

For ***HELP*** *on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network ☒

Title:	⌘	Combined CR to 23.234 Annex D (SMS over IP)
Source:	⌘	SA2
Work item code:	⌘	WLAN
Date:	⌘	20/5/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	This CR contains combined changes from CR31 (S2-041650), CR5 (S2-041544). CR31 and CR5 contain changes agreed by SA2 before approval of the TS but not implemented in the version sent for approval. Please see individual CRs for detailed reasons for change.
Summary of change:	⌘	This CR contains combined changes from CR31 (S2-041650), CR5 (S2-041544). See these CRs for details of the changes.
Consequences if not approved:	⌘	Combination of the CRs may not be implemented according to SA2 decision.

Clauses affected:	⌘	Annex D				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

**************************** Start of Changes *****************************

Annex D (~~informative~~normative) Short Message Service ~~Support of SMS~~ ~~over WLAN~~

D.1Architecture for support of SMS ~~over WLAN~~

The architecture for support of IP delivery and origination of SMS messages is illustrated in figure D.1. The SM-SC and GMSC/SMS-IWMSC are defined in TS 23.040 [6]. The IP Short Message Gateway IP-SM-GW communicates between the IP client and the GMSC/SMS-IWMSC. ~~When the WLAN UE is connected to and authenticated with the 3GPP network, the HLR/HSS shall be able to provide the address of the IP-SM-GW in order to enable the SMS message to be routed to the WLAN UE.~~

The intention of this architecture is that it could be realised through re-use of existing messaging protocols supported by the UE e.g. IMS or MMS. The primary purpose of this architecture desription is therefore to describe the interaction between the IP SM Gateway and the existing elements supporting the Short Message Service (GMSC/SMS-IWMSC, SM-SC and HLR/HSS).

The IP SM Gateway should be considered as consisting of all the functional entities needed to interwork between the chosen existing messaging protocol(s) and the existing SMS elements. For example, in the case IMS Messaging is chosen, the requirements on the IP SM Gateway specified here could be met by a combination of the CSCFs and an IMS Application Server which interworks to the GMSC/SMS-IWMSC.

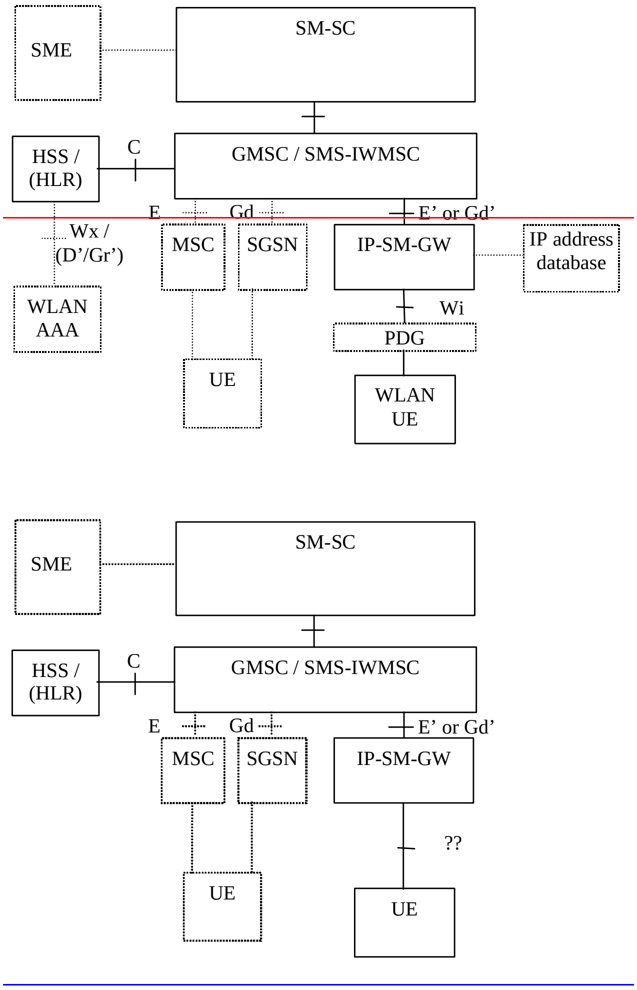


Figure D.1: Architecture for SMS ~~interworking~~ support with an IP attached terminal

D.1.1 IP Short Message Gateway (IP-SM-GW)

The IP-SM-GW shall provide the protocol interworking for delivery of the short message between the IP client and the GSM/UMTS network. The functions of this network element are:

- To connect to the GMSC using established MAP protocols over SS7, appearing to the GMSC as an MSC or SGSN using the E or Gd reference points
- To connect to the SMS-IWMSC using established MAP protocols over SS7, appearing to the GMSC as an MSC or SGSN using the E or Gd reference points
- To communicate with the IP client using IP based protocols maintaining the format and functionality of the SMS message. It is intended that existing messaging protocols supported by the UE should be reused for this purpose.
- To maintain the association between~~e~~ the MSISDN ~~with~~ and the IP address of the terminal
- Support registration and authentication of the ~~WLAN~~ UE for SMS services
- Support of security associations between ~~WLAN~~ UE and IP-SM-GW

D.1.2 HLR/HSS ~~enhancements~~

In the routeing of an SMS message, the SMS-GMSC performs a MAP request to the HLR/HSS “send routing information for short message” as defined in TS 29.002 [10] to determine the address of the MSC or SGSN to which to route the short message.

When the ~~WLAN~~ UE is connected only to a GSM/UMTS network, the “send routing information for short message” returns the address of the MSC or SGSN for delivery of SMS message. In the event that the ~~WLAN~~ UE is ~~connected via WLAN to the 3GPP network~~registered with an IP Short Message Gateway, the HLR/HSS may return the address of the IP-SM-GW in the “send routing information for short message”. As such, the HLR/HSS shall support the following functionality:

- An indication that the terminal is ~~IP connected~~registered with an IP Short Message Gateway (e.g. an internal flag) for delivery of SMS
- The SS7 MAP address of the IP-SM-GW
- The logic necessary to act on the fact that the terminal is IP connected and return the IP-SM-GW address

The mechanism for prioritizing whether the short message is delivered via a GSM/UMTS or a WLAN connection when the terminal is simultaneously connected to both access networks is outside the scope of this specification.

D.1.2.1~~ An i~~Indication that the terminal is ~~IP connected~~registered with an IP Short Message gateway

In order to be able to return the address of the IP-SM-GW in response to a “SendRoutingInfoForShortMsg” request from the GMSC, the HLR/HSS needs to have an indication that the terminal is ~~IP connected~~registered with an IP Short Message Gateway and that this is the preferred method for delivery of short messages.

The ~~3GPP AAA server~~IP Short Message Gateway maintains the ~~WLAN~~ UE’s ~~WLAN attach~~registration status. On ~~attachment~~registration, the ~~AAA server~~IP Short Message Gateway shall send a message to the HLR/HSS ~~when the UE is WLAN IP attached~~indicating that the UE has sucessfully registered~~ and authenticated and when it is detached~~.

D.1.2.2 The address of the IP-SM-GW

The address of the IP-SM-GW associated with a registered ~~WLAN~~ UE may either be pre-defined as a single address in the HLR/HSS or dynamically configured during the registration process, depending on information received~~ from the 3GPP AAA server or~~ from the IP-SM-GW~~ itself~~.

~~D.1.3 IP address database~~

~~The IP address database shall contain the mapping of the IP address of the terminal with the cellular MSISDN. This database may be in the HLR/HSS, in a AAA server or in a ENUM server or it may be contained within the IP-SM-GW. The database is populated during SMS service registration and authentication of the WLAN UE.~~

NOTE: In the context of WLAN, the IP address of the WLAN UE is the remote IP address.

D.1.~~4~~3 Reference points

The need for additional reference points is for further study.

~~D.1.5 IP Connectivity for SMS over WLAN~~

~~For delivery of SMS over WLAN, the WLAN UE needs IP connectivity. WLAN UE gets the IP connectivity by establishing a tunnel to an appropriate home network PDG. The registration of WLAN UE for SMS services occurs over this tunnel. This tunnel shall be maintained for use with SMS services while the WLAN UE is registered with IP-SM-GW. It will be used for sending or receiving of any SMS messages to and from the WLAN UE.~~

D.2 Procedures

D.2.1 Registration with IP Short Message Gateway

D.2.1.1 General

Before originating or receiving SMS messages over IP, the UE must register with an appropriate IP Short Message Gateway.

The registration process shall:

- Provide mutual authentication between UE and IP Short Message Server
- Provide for authorisation of the UE for the SMS service
- Establish registration state for the UE within the IP Short Message Server

On completion of registration the IP Short Message Gateway shall inform the HLR/HSS that the user has registered.

NOTE: This registration may be implicitly provided through registration to an existing messaging service which is providing interworking to SMS (assuming SMS interworking is allowed according to the user's subscription).

D.2.1.2 Information flows for registration

FFS.

D.2.2 De-registration from the IP Short Message Gateway

D.2.2.1 General

De-registration of the UE from the IP Short Message Gateway may be triggered by an explicit UE-initiated deregistration procedure with the IP SM GW or automatically by the IP SM GW on SMS delivery failure.

The explicit UE-initiated de-registration procedure may be used when the UE is aware that it is about to loose IP connectivity or when the terminal is shut down.

After de-registration, the IP SM GW shall inform the HLR so that subsequent SMS messages shall be delivered instead over the CS or PS domain.

NOTE: This de-registration may be implicitly provided through de-registration from an existing messaging services which is providing SMS interworking.

D.2.2.2 Information flows for UE-initiated de-registration

FFS.

D.2.2.3 Information flows for automatic de-registration

FFS.

D.2.3 Delivery of short messages

~~D.2 Delivery of short messages to WLAN (IP) connected client~~

An SMS message destined for a particular terminal (with a destination address identified by a MSISDN) is originated by an SME and is sent to the SM-SC associated with that SME in accordance with TS 23.040 [6]).

D.2.3.1 Message Information flows for IP terminated short messages

The ~~message~~ information ~~sequence~~ flow for transport of the IP terminated short message from the short message service centre (SM-SC) to the IP client on the ~~WLAN~~ UE is shown in figure D.2.

The SMS may either be delivered directly to the ~~WLAN~~ UE once the IP-SM-GW has received the short message (direct method), or alternatively a notification may be used (notification method). In the notification method, the IP-SM-GW sends a message to the ~~WLAN~~ UE that a short message is available and awaits a response from the ~~WLAN~~ UE to determine if the user wishes to receive the message.

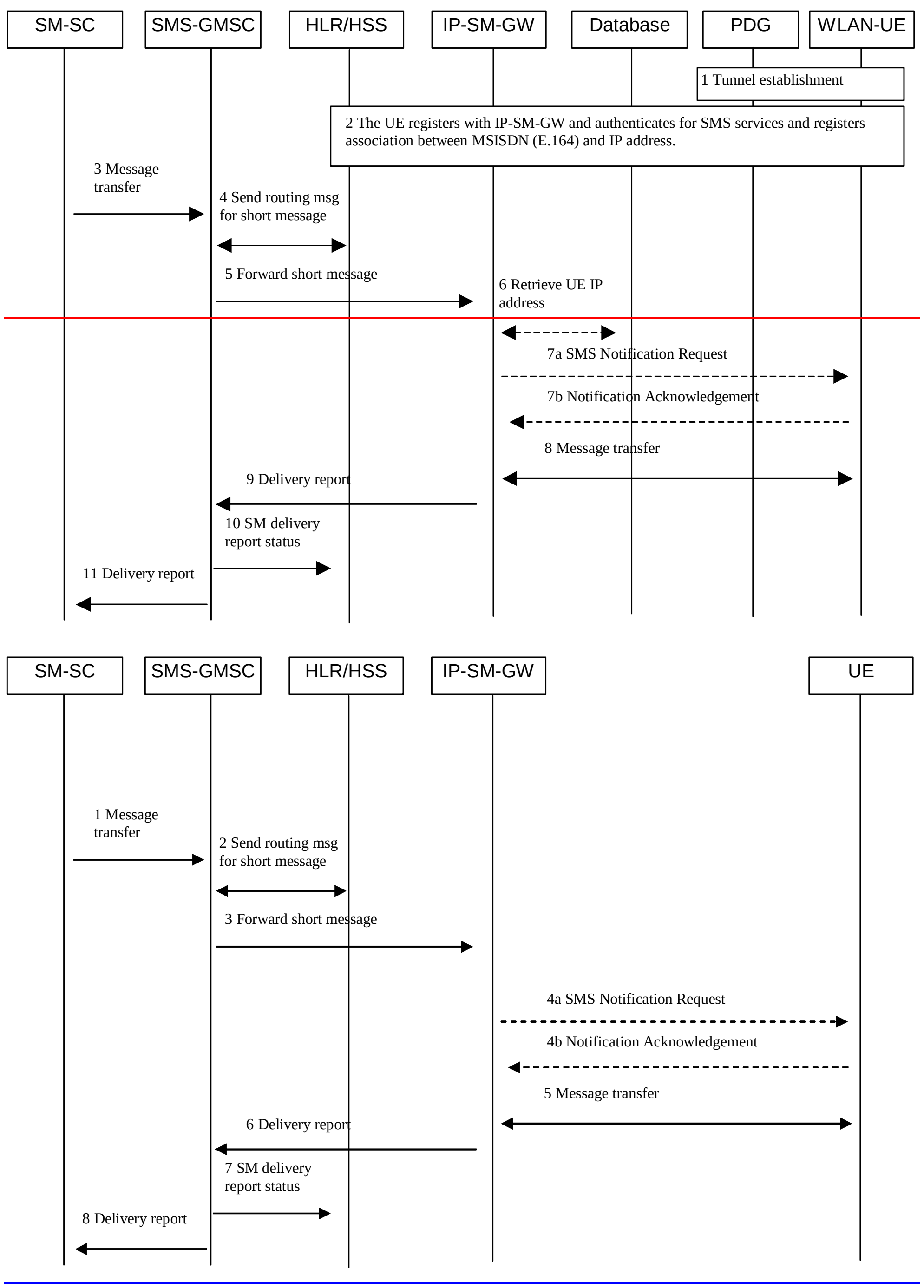

SM-SC
SMS-GMSC
HLR/HSS
IP-SM-GW
Database
PDG
WLAN-UE
1 Tunnel establishment
2 The UE registers with IP-SM-GW and authenticates for SMS services and registers association between MSISDN (E.164) and IP address.
3 Message transfer
4 Send routing msg for short message
5 Forward short message
6 Retrieve UE IP address
7a SMS Notification Request
7b Notification Acknowledgement
8 Message transfer
9 Delivery report
10 SM delivery report status
11 Delivery report
SM-SC
SMS-GMSC
HLR/HSS
IP-SM-GW
UE
1 Message transfer
2 Send routing msg for short message
3 Forward short message
4a SMS Notification Request
4b Notification Acknowledgement
5 Message transfer
6 Delivery report
7 SM delivery report status
8 Delivery report

Figure D.2: SMS delivery to IP terminal

~~1)The tunnel between the WLAN UE and the home PDG is established.~~

~~2)Following establishment of the tunnel, the WLAN-UE registers with IP-SM-GW establishing any necessary security association, authenticates for support of SMS services and registers the association between the UE MSISDN (E.164) and its IP address~~

~~3)~~1) The SM-SC forwards the SMS message to the GMSC

~~4)~~2) The GMSC interrogates the HLR/HSS to retrieve routeing information sendRoutingInfoForShortMsg for the ~~WLAN~~ UE. When a user is registered on a WLAN network for delivery of SMS messages, the HLR/HSS returns the address of IP-SM-GW (rather than address of appropriate MSC or SGSN)

~~5)~~3) GMSC delivers the SMS to IP-SM-GW using protocols as if it was a message to an MSC or SGSN.

~~6)Optionally, the IP-SM-GW interrogates the database to identify the IP address and relevant security parameters associated with the WLAN UE.~~

4~~7~~a) When notification method of delivery is used, the IP-SM-GW sends an SMS notification request to the ~~WLAN~~ UE to inform it that an SMS message is available for delivery.

~~7b~~4b) When notification method of delivery is used, on receipt of the SMS notification message, the UE responds with a notification acknowledgement indicating whether it wishes to receive the SMS message.

~~8.~~5) ~~I~~n the event that the direct method of delivery is used, or that a positive acknowledgement is received from the ~~WLAN~~ UE in response to the SMS notification request, the IP-SM-GW delivers SMS to IP client using e.g. WAP, SMPP, MMAP, XML, SIP (e.g. IMS client), SMTP, IMAP.

~~9.~~6) IP-SM-GW sends delivery report back to SMS-GMSC (see TS 23.040 [6])

~~10.~~7) SMS-GMSC sends SM delivery report to HLR/HSS (see TS 23.040 [6])

~~11.~~8) SMS- GMSC sends SM delivery report to SM-SC (see TS 23.040 [6])

Error handling is performed using the mechanisms defined in TS 23.040 [6]**Error! Reference source not found.**.

D.2.4~~3~~ Short message~~s~~ origination ~~ed on WLAN (IP) connected client~~

An SMS message destined for a particular terminal (with a destination address identified by a MSISDN) may be originated by the ~~WLAN (IP) attached client~~UE and sent, ~~via the PDG in the case of WLAN,~~ to the IP-SM-GW using an IP based protocol.

D.~~3~~2.4.1 Message Information flow for IP originated short messages

The ~~message~~ information ~~sequence~~ flow for transport of the IP originated short message to the short message service centre (SM-SC) is shown in figure D.3. This is based on the message sequence flow in TS 23.040 [6], maintaining where possible the existing message sequences.

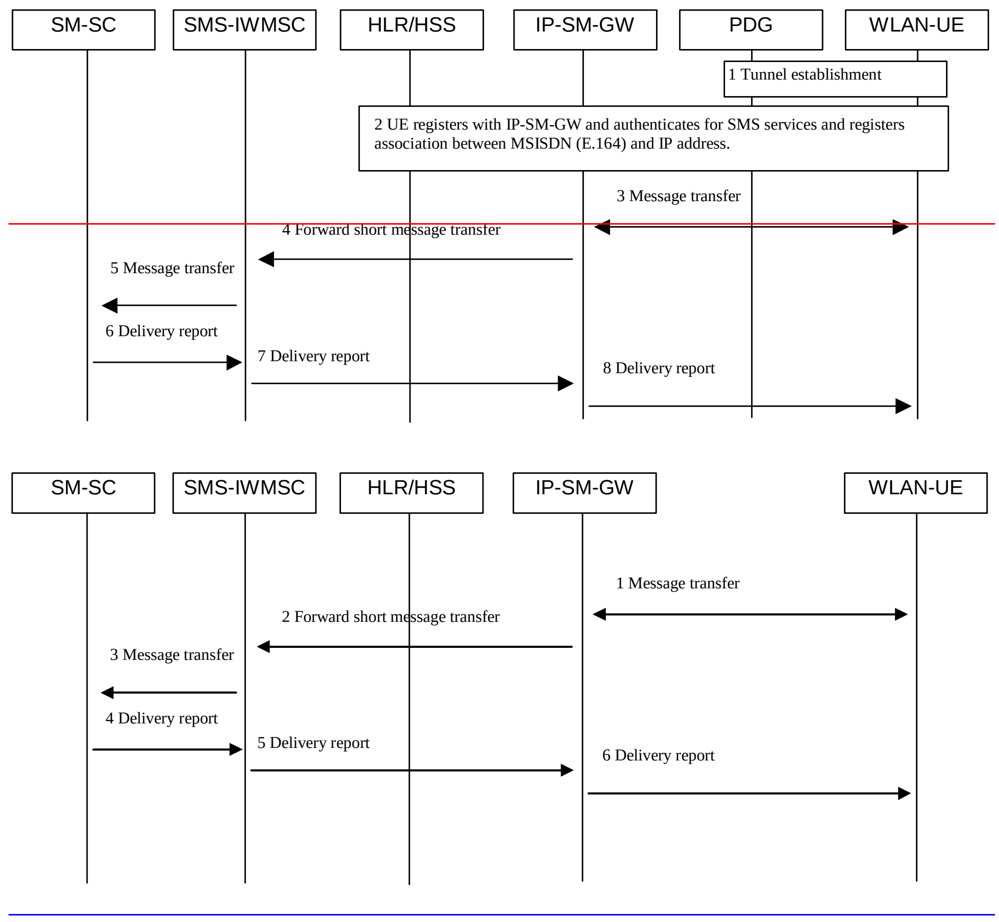


Figure D.3: SMS origination from IP terminal

~~1)The tunnel between the WLAN UE and the home PDG is established.~~

~~2)Following establishment of the tunnel, the WLAN UE registers with IP-SM-GW establishing any necessary security association, authenticates for support of SMS services and registers the association between the WLAN UE MSISDN (E.164) and its IP address~~

~~3)~~1) IP client delivers SMS message to the IP-SM-GW, using e.g. WAP, SMPP, MMPP, XML, SIP, SMTP.

~~4)~~2) IP-SM-GW extracts the SMS message and forwards it to SMS-IWMSC using standard MAP (as TS 23.040) exactly as if it was an MSC or SGSN.

~~5)~~3) The SMS-IWMSC forwards the SMS message to the SM-SC (see TS 23.040 [6]))

~~6)~~4) SM-SC sends delivery report SMS-IWMSC (see TS 23.040 [6])

~~7)~~5) SMS-IWMSC sends delivery report to IM-SM-SC (see TS 23.040 [6])

~~8)~~6) IP-SM-GW sends delivery report to IP-UE ~~using proprietary mechanism and/or protocols~~.

Error handling is performed using the mechanisms defined in TS 23.040 [6].

D.3Support of SMS over WLAN interworking

This subclause describes the use of the above mechanism with the WLAN interworking system. For this purpose, the WLAN-UE needs IP connectivity. The WLAN-UE gets IP connectivity by establishing a tunnel to an appropriate home network PDG. The registration of WLAN-UE for SMS services occurs over this tunnel. This tunnel shall be maintained for use with SMS services while the WLAN-UE is registered with IP-SM-GW. It will be used for sending or receiving of any SMS messages to and from the WLAN-UE.

Figure 8.4 below shows a complete call flow, from WLAN tunnel establishment through SMS registration to the sending of an SMS by the UE. Note that Tunnel Establishment and registration with an IP-SM gateway may occur some time before a message needs to be sent since the UE also needs to be registered with the IP-SM-GW in order to receive SMS messages.

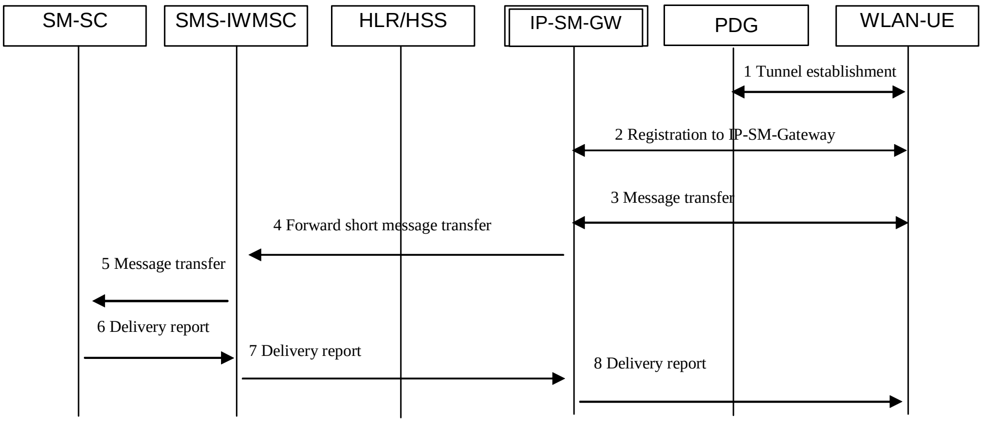


Figure D.4: Complete SMS call flow with WLAN interworking

************************** End of Changes *****************************